D-Link® DFL-500

SOHO Firewall

User’s Manual

Rev. 02 (March, 2002)

D-Link Systems, Inc.

© Copyright 2002 D-Link Systems, Inc. All rights reserved.

No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of D-Link Systems, Inc.

DFL-500 User Manual
Version 2.2
30 March 2002

Trademarks
Products mentioned in this document are trademarks or registered trademarks of their respective holders.

Regulatory Compliance
FCC Class A Part 15 CSA/CUS

Table of Contents

Introducing the DFL-500 9

Firewall 9
Network Address Translation (NAT) 9
Transparent mode 10
Hacker prevention and protection 10
VPN 10
Virus and worm protection 11
Web content filtering 11
Secure installation, configuration, and management 12
Web-based manager 12
Command line interface 12
Logging and reporting 12
About this document 13
Customer service and technical support 13

Installing the DFL-500 14

Before you start 14
NAT mode install 14
Transparent Mode Install 15
Unpacking the DFL-500 16
Mounting the DFL-500 16
Powering on the DFL-500 17
Using the firewall setup wizard 17
Connecting to the web-based manager 17
Starting the firewall setup wizard 18
Reconnecting to the web-based manager 18
Completing your PPPoE configuration 18
Configuring the DFL-500 from the CLI 19
Connecting to the CLI 19
Configuring the DFL-500 to run in NAT mode 19
Configuring the DFL-500 to run in Transparent mode 20
Connecting the DFL-500 to your network 21
Configuring your internal network 22
Completing the configuration 22
Setting the date and time 22

Firewall Configuration 23

Policies 23
Types of policies 23
Policy information 24
Default policy 24

Adding policies 24
Editing policies 26
Policy matching 26
Arranging policies in the policy list 26
Controlling connections from the Internet 26
Accepting incoming connections in NAT mode 27
Accepting incoming connections in Transparent mode 27
Denying incoming connections 27
Controlling connections to the Internet 28
Denying connections to the Internet from the internal network 28
Accepting connections to the Internet from the internal network 29
Requiring authentication to connect to the Internet 30
Addresses 31
Adding addresses 31
Editing addresses 32
Services 32
Pre-defined services 32
Providing access to custom services 33
Grouping services 34
Schedules 35
Creating one-time schedules 35
Creating recurring schedules 36
Applying a schedule to a policy 37
Users and authentication 37
Adding user names and passwords 38
Setting authentication time out 38
Adding authentication to a policy 38
Virtual IPs 39
Adding Virtual IPs 39
IP/MAC binding 40
Adding IP/MAC binding addresses 40
Enabling IP/MAC binding 40
Traffic shaping 41
Adding traffic shaping to a policy 41

IPSec VPNs 42

Compatibility with third-party VPN products 42
Autokey IPSec VPN between two networks 43
Creating the VPN tunnel 44
Adding internal and external addresses 45
Adding an IPSec VPN policy 46
Autokey IPSec VPN for remote clients 47
Configuring the VPN tunnel for the client VPN 48
Adding internal and external addresses 49

Adding an IPSec VPN policy 49
Configuring the IPSec VPN client 50
Manual key exchange IPSec VPN between two networks 50
Configuring the VPN tunnel 50
Adding internal and external addresses 51
Adding an IPSec VPN policy 52
Manual key exchange IPSec VPN for remote clients 52
Configuring the VPN tunnel 52
Adding internal and external addresses 52
Adding an IPSec VPN policy 52
Testing a VPN 53
IPSec VPN pass through 53
IPSec client to network VPN pass through 53
IPSec network to network VPN pass through 54

PPTP and L2TP VPNs 56

PPTP VPN configuration 56
Configuring the DFL-500 as a PPTP server 57
Configuring a Windows 98 client for PPTP 58
Configuring a Windows 2000 Client for PPTP 59
Configuring a Windows XP Client to connect to a DFL-500 PPTP VPN 59
PPTP VPN pass through 60
PPTP client to network VPN pass through 61
L2TP VPN configuration 62
Configuring the DFL-500 as an L2TP server 62
Configuring a Windows 2000 Client for L2TP 63
Configuring a Windows XP Client to connect to a DFL-500 L2TP VPN 64
RADIUS authentication for PPTP and L2TP VPNs 66
Adding RADIUS server addresses 66
Turning on RADIUS authentication for PPTP 67
Turning on RADIUS authentication for L2TP 67

Intrusion detection system (IDS) 68

Attack prevention 68
Alert email 68
Configuring alert email 69
Testing email alerts 69

Virus protection 70

Virus protection for your internal network 70
High level virus protection for your internal network 71
Medium level virus protection for your internal network 72
Low level virus protection for your internal network 73
Virus protection for incoming connections 73
High level virus protection for incoming connections 74

Medium level virus protection for incoming connections 74
Low level virus protection for incoming connections 75
Worm protection 75
Worm protection for your internal network 76
Worm protection for incoming connections 76
Updating your antivirus database 76
Manual antivirus database updates 77
Automatic antivirus database updates 77
Displaying virus and worm lists 78

Web content filtering 79

Block web pages that contain unwanted content 79
Enabling the banned word list 79
Adding words to the banned word list 79
Temporarily disabling the banned word list 80
Temporarily disabling individual words in the banned word list 80
Clearing the banned word list 80
Creating the banned word list using a text editor 80
Block access to Internet sites 81
Enabling the URL block list 81
Adding URLs to the URL block list 81
Temporarily disabling the URL block list 82
Temporarily disabling blocking individual URLs 82
Clearing the URL block list 82
Creating the URL block list using a text editor 82
Remove scripts from web pages 83

Logging and reporting 84

Configuring logging 84
Recording logs on a remote computer 84
Selecting what to log 85
Log message formats 85
Traffic log message format 86
Event log message format 86
Attack log message format 87

Administering the DFL-500 88

Logging into the web-based manager 88
System status 89
Changing the operating mode 89
Upgrading the DFL-500 firmware 89
Updating your antivirus database 89
Displaying the DFL-500 serial number 90
Backing-up system settings 90
Restoring system settings 90

Restoring system settings to factory defaults 90
Restarting the DFL-500 92
Shutting down the DFL-500 92
System status monitor 92
Network configuration 93
Changing IP addresses 93
Configuring the external interface for DHCP 93
Configuring the external interface for PPPoE 93
Changing MTU size to improve network performance 94
Setting DNS server addresses 94
Controlling management access to the DFL-500 94
Configuring routing 95
Enabling RIP server support 95
Providing DHCP services to your internal network 96
System configuration 97
Setting system date and time 97
Changing web-based manager options 98
Adding and editing administrator accounts 98
Configuring SNMP 100

Using the DFL-500 CLI 101
Connecting to the DFL-500 CLI 101
Connecting to the DFL-500 communications port 101
Connecting to the DFL-500 CLI using SSH 102
CLI basics 102
Recalling commands 103
Editing commands 103
Using command shortcuts 103
Using command help 103
Installing firmware from a TFTP server 103

Glossary 106

Troubleshooting FAQs 109
General administration 109
Network configuration 109
Firewall policies 109
Schedules 110
VPN 110
Virus protection 111
Web content filtering 111
Logging 111

Technical Support 112

Introducing the DFL-500

The DFL-500 is one of a series of new generation all-layer security products that provide comprehensive protection for your internal network. These products, Application Security Gateways, combine key security technologies into a dedicated platform designed for high performance and reliability. In a compact, easy to install and configure package the DFL-500 combines:

- A fully-configurable firewall
- Hacker attack prevention and protection
- Virtual private networking (VPN)
- Virus protection
- Content filtering
- Easy and secure configuration management

Easily installed using the web-based manager firewall setup wizard, the DFL-500 is up and running in minutes, providing comprehensive protection and content control for your small office/home office (SOHO) network.

Firewall

The core function of the DFL-500 is a state-of-the-art firewall that protects computer networks from the hostile environment of the Internet. The firewall provides control of security policies through a carefully designed interface that is easy to use but allows full control even in complex situations.

DFL-500 security policies include a complete range of options that:

- Control incoming and outgoing traffic
- Block or allow access for all policy options
- Control when individual policies are in effect
- Accept or deny traffic to and from individual addresses
- Control standard and user definable network services individually or in groups
- Require users to enter passwords before gaining access to the Internet
- Include traffic shaping to set priority and guarantee or limit bandwidth for each policy

Network Address Translation (NAT)

In NAT mode, the DFL-500 is installed as a privacy barrier between the private network and the Internet. The firewall provides network address translation to protect the private network. In NAT mode, you can add a Internal network to provide public access to Internet servers while protecting them behind the firewall on a separate internal network.

Features supported in NAT mode include:

- Firewall protection, allow/deny traffic according to source/destination address, service, time of day, etc.
- VPN, virus protection, and Web content filtering
- IP/MAC binding
- DHCP configuration of the DFL-500 external network address
- Detailed logging features

Transparent mode

Transparent Mode provides even quicker and easier installation when the requirement is to provide firewall protection to a pre-existing network with public addresses. The internal and external network interfaces of the DFL-500 can be in the same network; therefore, the DFL-500 can be inserted into your network at any point without the need to make any changes to your network.

Packets arriving at the DFL-500 are intelligently forwarded to the correct network interface and firewall policies prevent unauthorized access to your network.

Transparent mode provides the same basic firewall protection as NAT mode. However, more advanced features such as the VPN, virus scanning, and content filtering are only available in NAT mode.

Hacker prevention and protection

The DFL-500 is built to defend your network from network attacks including:

- Distributed Denial-Of-Service (DDOS) attacks
  SYN Attack
  ICMP Flood
  UDP Flood
- IP fragmentation attacks
  Ping of Death Attack
  Tear Drop Attack
  Land Attack
- Port Scan Attack
- IP Source Routing
- IP Spoofing Attack
- Address Sweep Attack
- WinNuke Attack

You can configure email alerts that send an email to the system administrator when the DFL-500 detects one of these attacks. You can also configure email alerts to provide real time warnings of ongoing attacks. Up to three email recipients can be specified.

VPN

Using the DFL-500 integrated VPN, you can provide a secure connection between widely separated office networks or securely link telecommuters or travellers to your office network. The DFL-500 industry standard VPN creates an encrypted traffic tunnel between DFL-500-protected networks or between a DFL-500 and third-party VPN products that support IPSec. VPN features include:

- IPSec, ESP security in tunnel mode
- Hardware accelerated encryption using IPSEC, DES, and 3DES (triple-DES)
- HMAC MD5 or HMAC SHA authentication and data integrity
- Automatic IKE (Internet Key Exchange) and manual key exchange
- PPTP for easy connectivity with the VPN standard supported by the most popular operating systems
- L2TP for easy connectivity with a more secure VPN standard also supported by many popular operating systems

- IPSec and PPTP VPN pass through so that computers or subnets on your internal network can connect to a VPN gateway on the Internet

Virus and worm protection

D-Link's DFL-500 secure gateway solution adds anti-virus and anti-worm functionality to conventional VPN and firewall security. Virus and worm protection screens the information found in web (HTTP protocol) and email content (SMTP, POP3, and IMAP protocols) for the following types of target files:

- Executable files (exe, bat, and com)
- Visual basic files (vbs)
- Compressed files (zip, gzip, tar, hta, and rar)
- Screen saver files (scr)
- Dynamic link libraries (dll)
- MS Office files

You can configure DFL-500 virus scanning to block the target files or scan them for viruses and worms. You can configure three levels of virus protection:

- High level protection removes target files from HTTP transfers and email attachments before they pass through the firewall

  With high level protection turned on, the DFL-500 does not perform virus scanning. Instead, all files and attachments are identified and removed from content protocol data streams.
- Medium level protection scans all target files for viruses

  You can configure the virus scanning engine to perform up to four different types of virus scans on each target file.
- Low level protection temporarily suspends virus protection

  All target files are forwarded unchanged to their destinations.

You can also configure worm scanning to look for filenames known to be used by worms. For example, the Nimda worm uses files named readme.exe and sample.exe.

DFL-500 content virus and worm prevention is transparent to the end user. Client and server programs require no special configuration, and D-Link high-performance hardware and software ensure there are no noticeable download delays.

Web content filtering

Using Web content filtering, you can screen for three types of web content:

- Unwanted content such as adult sites
- Unwanted URLs such as stock quote/trading sites
- Unsecure web content such as:

  Java Applets
  Cookies
  Malicious Scripts
  ActiveX

Site blocking is accomplished by scanning URLs or web pages for user defined patterns.

Secure installation, configuration, and management

Installation is quick and simple. All that is required to get the DFL-500 up and running and protecting your network is to connect to the web-based manager and use the firewall setup wizard. You can also do the basic configuration from the DFL-500 command line interface (CLI).

When initially connected to your network, the DFL-500 comes with a default configuration that provides basic security features. From this foundation you can use the web-based manager to customize the configuration to meet your needs.

Web-based manager

Using a secure HTTPS connection from any computer running Internet Explorer, you can configure and manage the DFL-500. It can also be configured for secure administration from the external network (Internet).

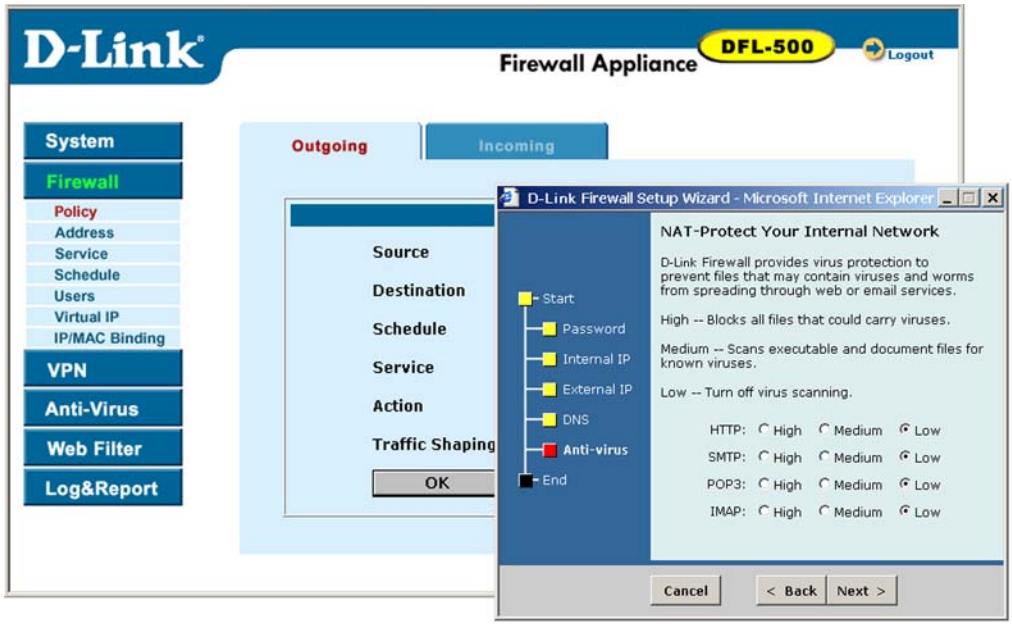
Configuration changes made with the web-based manager are effective immediately without the need to reset the firewall or interrupt service.

Once a satisfactory configuration has been established, it can be downloaded and saved. The saved configuration can be restored at any time.

Command line interface

For troubleshooting and professional scripting, a command line interface is available by connecting a management computer to the DFL-500 RS-232 serial connection.

The DFL-500 web-based manager:



Logging and reporting

The DFL-500 supports logging of various categories of traffic and of configuration changes. You can configure logging to:

- Report traffic that connects to the firewall interfaces
- Report network services used
- Report traffic permitted by firewall policies

- Report traffic that was denied by firewall policies
- Report configuration changes

Logs can be sent to a remote syslog server.

About this document

This user manual describes how to install and configure the DFL-500. This document contains the following information:

- Installing the DFL-500
- Firewall configuration describes how to configure firewall policies to enhance firewall protection
- IPSec VPNs describes how to create an IPSec VPN between two internal protected networks and between an internal network and a client
- PPTP and L2TP VPNs describes how to configure PPTP and L2TP VPNs between the DFL-500 and a windows client
- Intrusion detection system (IDS) describes how to configure the DFL-500 to detect and prevent common network attacks
- Virus protection describes how use the DFL-500 to protect your network from viruses and worms
- Web content filtering describes how to configure web content filters to prevent unwanted Web content from passing through the DFL-500
- Logging and reporting describes how to configure logging and reporting to track activity through the DFL-500
- Administering the DFL-500 describes DFL-500 management and administrative tasks
- Using the DFL-500 CLI introduces the DFL-500 CLI and describes the basics of connecting to and using the CLI
- The Glossary defines many of the terms used in this document
- Troubleshooting FAQs help you find the information you need if you run into problems

Customer service and technical support

For updated product documentation, technical support information, and other resources, please visit our web site at http://tsd.dlink.com.tw

You can contact D-Link Technical Support at your local D-Link office:

- See Technical Support

To make it possible for us to provide the support you require, please provide the following information:

- Name
- Company Name
- Location
- Email address
- Telephone Number
- Software Version
- Serial Number
- Detailed description of your problem

Installing the DFL-500

This chapter describes how to install the DFL-500 firewall between your network and the Internet. After you have completed the procedures in this chapter, your DFL-500 will be up and running and protecting your internal network.

This chapter includes:

- Before you start
- Unpacking the DFL-500
- Mounting the DFL-500
- Powering on the DFL-500
- Using the firewall setup wizard
- Configuring the DFL-500 from the CLI
- Connecting the DFL-500 to your network
- Configuring your internal network
- Completing the configuration

Before you start

Before starting the installation of the DFL-500, you must decide whether you are going to be running it in NAT mode or Transparent mode. This choice determines the information that you require to install the DFL-500 as well as the installation steps that you perform.

NAT mode install

Use NAT mode configuration information to collect the information required to configure the DFL-500 to run in Network Address Translation (NAT) mode.

NAT mode configuration information (Part 1 of 2)

1. Administrator Password	Create an administrator password. The password should be difficult to guess. It must be at least 6 characters long and can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and the @ character are not allowed.				
2. Internal Interface	In the space below, record the IP address and netmask to connect the DFL-500 to your internal network.				
IP*		**Netmask**			
3. External Interface	If your ISP has assigned you a static IP address, put a check mark next to Manual below. Record the Manual IP address and netmask to connect the DFL-500 to the internet and record the IP address of your default internet IP gateway. If your ISP supplies you with an IP address using DHCP or PPPoE, check the appropriate box below. Record the IP address of your default Internet gateway as assigned by your ISP.				
	Manual		**DHCP**		PPPoE	
IP*		**Mask**			
Gateway					

PPPoE User Name			**Password**			
4. DNS Server	In the space below, record the IP addresses of the primary and secondary DNS servers provided by your ISP.					
Primary			**Secondary**			
5. DHCP Server (optional)	If you plan to use the DFL-500 as a DHCP server to assign IP addresses to the computers on your internal network, you must specify the IP address range reserved to be assigned by the DHCP server.					
Starting IP			**Ending IP**			
6. Protect Your Internal Network (optional)	Choose virus protection levels to protect your internal network from viruses. You can set high, medium, and low protection for web traffic (HTTP), and email traffic (SMTP, POP3, and IMAP). For information on high, medium, and low protection, see Virus protection. Turn on incoming or outgoing worm protection. For information worm protection, see Worm protection.					
HTTP	**High**		**Medium**		**Low**	
SMTP	**High**		**Medium**		**Low**	
POP3	**High**		**Medium**		**Low**	
IMAP	**High**		**Medium**		**Low**	
Worm Protection	**Incoming**		**Outgoing**			
* The Internal and External IP addresses must be on separate subnets.						

Transparent Mode Install

Use Transparent mode configuration information to collect the information required to configure the DFL-500 to run in Transparent mode.

Transparent mode configuration information			
1. Administrator Password	Specify an administrator password. The password should be difficult to guess. It must be at least 6 characters long and can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and the @ character are not allowed.		
2. Transparent Management IP	In the space below, record the IP address and netmask to connect the DFL-500 to a network for management. Management can be done from a computer on your internal network or from a separate network. Also record the IP address of the default gateway required to connect the DFL-500 to a network for management. The default gateway address is not required if the management computer can be reached without going through a default gateway.		
Management IP		**Netmask**	
Default Gateway			
3. DNS Server	In the space below, record the IP addresses of the primary and secondary DNS servers provided by your ISP.		

Primary		Secondary	

Unpacking the DFL-500

The DFL-500 package contains the following items:

- The DFL-500 firewall
- A blue cross-over ethernet cable
- A gray regular ethernet cable
- A null-modem cable
- The DFL-500 Quick Start Guide
- A CD containing this *DFL-500 User Manual*
- A AC adapter

DFL-500 package contents

Mounting the DFL-500

The DFL-500 can be installed on any stable surface. Make sure the appliance has at least 1.5 in. (3.75 cm) of clearance on each side to allow for adequate air flow and cooling.

Dimensions

- 219 x 156 x 35 mm

Weight

- 1.5 lb.

Power requirements

- DC input voltage: 5 V
- DC input current: 3 A

Environmental specifications

- Operating Temperature: 32 to 104 °F (0 to 40 °C)
- Storage Temperature: -13 to 158 °F (-25 to 70 °C)
- Humidity: 5 to 95% non-condensing

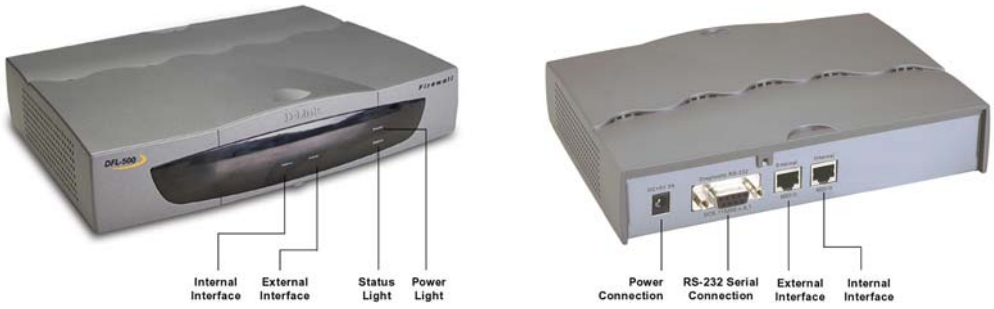
Powering on the DFL-500

To power on the DFL-500:

- Connect the power cord to the power connection at the back of the DFL-500.
- Connect the power cord to a power outlet.

The DFL-500 starts up. The Power and Status lights light. The Status light flashes while the DFL-500 is starting up and remains lit when the system is up and running.

Front and back view of the DFL-500



Using the firewall setup wizard

Use the procedures in this section to connect to the web-based manager and use the firewall setup wizard to create your initial DFL-500 configuration.

Connecting to the web-based manager

To connect to the web-based manager you require:

  - A computer with an ethernet connection
  - Internet Explorer version 4.0 or higher
  - A crossover cable or an ethernet hub and two ethernet cables

- Set the IP address of the computer with an ethernet connection to the static IP address 192.168.1.2 and a netmask of 255.255.255.0.
- Using the crossover cable or the ethernet hub and cables, connect the Internal interface of the DFL-500 to the computer ethernet connection.
- Start Internet Explorer and browse to the address ***https://192.168.1.99*** .

  The DFL-500 login page appears.
- Type admin in the Name field and click Login.

DFL-500 login page

Starting the firewall setup wizard

To start the firewall setup wizard:

Click the Wizard button at the upper right of the web-based manager.

- Select the operating mode: Network Address Translation (NAT) or Transparent.
- If you selected Network Address Translation (NAT), use the information that you gathered in NAT mode configuration information to fill in the wizard fields. Click the next button to step through the wizard pages.

  If you selected Transparent, use the information in Transparent mode configuration information to fill in the wizard fields. Click the next button to step through the wizard pages.
- Confirm your configuration settings and then click Finish and Close.

Reconnecting to the web-based manager

If you changed the IP address of the internal interface or switched to Transparent mode while using the firewall setup wizard, you must reconnect to the web-based manager using a new IP address:

- In NAT mode if you changed the IP address of the internal interface, browse to https:// followed by the new IP address of the internal interface
- In Transparent mode, browse to https:// followed by the Transparent mode Management IP address

Otherwise, you can reconnect to the web-based manager by browsing to https://192.168.1.99.

Completing your PPPoE configuration

If you configured the external interface to use PPPoE you must add your PPPoE user name and password. From the web-based manager:

- Go to *System* > *Network* > *IP Address* .
- Click and type your PPPoE user name and password.
- Click OK.

You have now completed the initial configuration of the DFL-500, and you can proceed to connect the DFL-500 to your network using the information in Connecting the DFL-500 to your network.

Configuring the DFL-500 from the CLI

To connect to the DFL-500 command line interface (CLI) you require:

- A computer with an available communications port
- A null modem cable with a 9-pin connector to connect to the communications port on the back panel of the DFL-500
- Terminal emulation software such as HyperTerminal for Windows

The following procedure describes how to connect to the DFL-500 CLI using Windows HyperTerminal software. You can use any terminal emulation program.

Connecting to the CLI

- Connect the null modem cable to the communications port of your computer and to the communications port on the back of the DFL-500.
- Make sure the DFL-500 is powered on.
- Start HyperTerminal, enter a name for the connection, and click OK.
- Specify the communications port in the Connect using field and click OK.
- Select the following port settings and click OK:

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

- Press Enter to connect to the DFL-500 CLI.

  The following prompt appears:

  ```
  D-Link login:
  ```

- Type `admin` and press Enter.

  The following prompt appears:

  ```
  Type ? for a list of commands.
  ```

Use the procedures that follow to configure the DFL-500 for NAT mode or Transparent mode operation. The NAT mode and Transparent mode procedures are different. Choose the correct ones for your installation. The NAT mode configuration procedures start next. The Transparent mode configuration procedures begin at Configuring the DFL-500 to run in Transparent mode.

Configuring the DFL-500 to run in NAT mode

The procedures in this section describe how to use the CLI to configure the DFL-500 to run in NAT mode.

Configuring NAT mode IP addresses

- Login to the CLI if you are not already logged in.
- Set the IP address and netmask of the internal interface to the Internal IP Address and Netmask that you recorded in NAT mode configuration information. Enter:

  ```
  set system interface internal ip <IP Address> <Netmask>
  ```

  Example

```
set system interface internal ip 192.168.1.1 255.255.255.0
```

- Set the IP address and netmask of the external interface to the External IP Address and Netmask that you recorded in NAT mode configuration information.

  To set the Manual IP address and netmask, enter:

  ```
  set system interface external manual ip <IP Address> <Netmask>
  ```

  Example

  ```
  set system interface external manual ip 204.23.1.5 255.255.255.0
  ```

  To set the external interface to use DHCP enter:

  ```
  set system interface external dhcp
  ```

  To set the external interface to use PPPoE enter:

  ```
  set system interface external pppoe <user name> <password>
  ```

  Example

  ```
  set system interface external pppoe username password
  ```

- Confirm that the addresses are correct. Enter:

  ```
  get system interface
  ```

  The CLI lists the IP address and netmask settings for each of the DFL-500 interfaces as well as the mode of the external interface (manual, DHCP, or PPPoE).

Configure the NAT mode default gateway

- Login to the CLI if you are not already logged in.
- Set the default route to the Default Gateway IP Address that you recorded in NAT mode configuration information. Enter:

  ```
  set system route add 0.0.0.0 0.0.0.0 gw <IP Address> dev external
  ```

  Example

  ```
  set system route add 0.0.0.0 0.0.0.0 gw 204.23.1.2 dev external
  ```

  You have now completed the initial configuration of the DFL-500 and you can proceed to connect the DFL-500 to your network using the information in Connecting the DFL-500 to your network.

Configuring the DFL-500 to run in Transparent mode

The procedures in this section describe how to use the CLI to configure the DFL-500 to run in Transparent mode.

Changing to Transparent mode

- Login to the CLI if you are not already logged in.
- Switch to Transparent mode. Enter:

  ```
  set system status opmode 2
  ```

  After a few seconds, the following prompt appears:

  ```
  D-Link login:
  ```

- Type `admin` and press Enter.

  The following prompt appears:

  ```
  Type ? for a list of commands.
  ```

- Confirm that the DFL-500 has switched to Transparent mode. Enter:

  ```
  get system status
  ```

  The CLI displays the status of the DFL-500. The last line shows the current operation mode.

  ```
  Version:DFL-500 2.20,build016,020326
  virus-db:2.104(03/19/2002 14:10)
  Serial Number:FGT-502801021075
  Operation mode:transparent
  ```

Configuring the Transparent mode management IP address

- Login to the CLI if you are not already logged in.
- Set the IP address and netmask of the Management IP to the IP address and netmask that you recorded in Transparent mode configuration information. Enter:

  ```
  set system manageip ip <IP Address> <Netmask>
  ```

  Example

  ```
  set system manageip ip 10.10.10.2 255.255.255.0
  ```
- Confirm that the address is correct. Enter:

  ```
  get system manageip
  ```

  The CLI lists Management IP address and netmask.

Configure the Transparent mode default gateway

- Login to the CLI if you are not already logged in.
- Add a default route set to the Default Gateway IP Address that you recorded in Transparent mode configuration information. Enter:

  ```
  set system manageip gateway <IP Address>
  ```

  Example

  ```
  set system manageip gateway 192.168.1.20
  ```

  You have now completed the initial configuration of the DFL-500 and you can proceed to connect the DFL-500 to your network using the information in Connecting the DFL-500 to your network that follows.

Connecting the DFL-500 to your network

Once the initial configuration of the DFL-500 is complete, you can connect the DFL-500 between your internal network and the Internet. The connection procedures are the same whether you are running in NAT mode or Transparent mode.

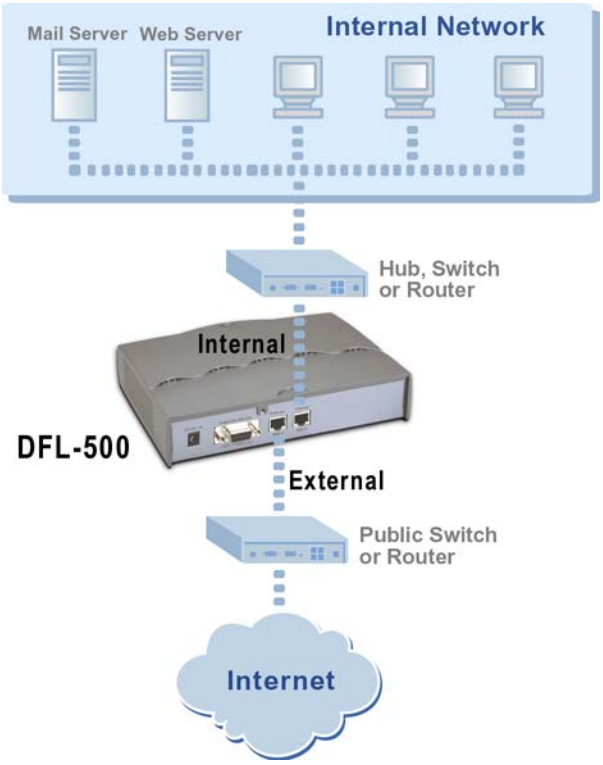
There are two 10/100 BaseTX connectors on the DFL-500:

- Internal for connecting to your Internal network
- External for connecting to your public switch or router and the Internet

To connect the DFL-500:

- Connect the Internal interface to the hub or switch connected to your internal network.
- Connect the External Interface to the public switch or router provided by your Internet Service Provider.

DFL-500 network connections:



Configuring your internal network

If you are running the DFL-500 in NAT mode, your internal network must be configured to route all internet traffic to the address of the internal interface of the DFL-500. This means changing the default gateway address of all computers and routers connected directly to the internal network.

If you are using the DFL-500 as the DHCP server for your internal network, configure the computers on your internal network for DHCP. Use the internal address of the DFL-500 as the DHCP server IP address.

If you are running the DFL-500 in Transparent mode, you do not have to make any changes to your network.

Once the DFL-500 is connected, make sure it is functioning properly by connecting to the Internet from a computer on your internal network. You should be able to connect to any Internet address.

Completing the configuration

Use the information in this section to complete the initial configuration of the DFL-500.

Setting the date and time

For effective scheduling and logging, the DFL-500 date and time should be accurate. You can either manually set the DFL-500 time or you can configure the DFL-500 to automatically keep its time correct by synchronizing with a Network Time Protocol (NTP) server.

To set the DFL-500 date and time, see Setting system date and time.

Firewall Configuration

This chapter describes how to use firewall policies to establish and control connectivity through the DFL-500 firewall. This chapter contains the following sections:

- Policies
- Controlling connections from the Internet
- Controlling connections to the Internet
- Addresses
- Services
- Schedules
- Users and authentication
- Virtual IPs
- IP/MAC binding
- Traffic shaping

Policies

By default the DFL-500 firewall allows all connections from the internal network to the Internet and blocks all connections from the Internet. Customizing the firewall configuration involves creating firewall policies to allow some connections that are blocked by default and to block or control some connections that are allowed by default. Before customizing the configuration of your DFL-500, you need to understand firewall policies.

Firewall policies are instructions that the firewall uses to decide what to do with a connection request. Policies contain information used to identify the characteristics of a connection request. Identifying information consists of the source address, destination address, and network service (or port number) used by the connection request. Identifying information also includes the time and date on which the firewall receives the connection request.

This section contains the following information about policies:

- Types of policies
- Policy information
- Default policy
- Adding policies
- Editing policies
- Policy matching
- Arranging policies in the policy list

Types of policies

In NAT mode you can create the following types of policies:

- Int to Ext that control connections from the Internal network to the Internet
- Incoming that control connections from the Internet to the internal network

In Transparent mode you can create the following types of policies:

- Outgoing that control connections from the Internal network to the Internet
- Incoming that control connections from the Internet to the internal network

Policy information

Policies direct the firewall to perform actions when a connection request matches the identifying information. A policy can specify that the firewall accepts, denies, or requests authentication for the connection. A policy can also trigger traffic log messages when the policy processes traffic and can apply traffic shaping to the traffic controlled by the policy.

The parts of a DFL-500 policy	
Identifying information	
Source Address	The IP address from which a user or service can connect to the firewall.
Destination Address	The location to which a user or service is attempting to connect when intercepted by the firewall.
Schedule	The time or date on which a policy is active.
Service	The network service to be provided through the firewall.
Action	
Action	The response of the firewall. The firewall can accept the connection, deny the connection, or require the user attempting to make the connection to provide authentication.
Log Traffic	Log Traffic adds messages to the traffic log whenever the policy processes traffic. For information about logging, see Logging and reporting.
Traffic Shaping	Traffic Shaping can be used to control the bandwidth available to, and set the priority of the traffic processed by the policy. For more information about traffic shaping, see Traffic shaping

Default policy

The default policy accepts connections from all computers at any source address on the internal network and grants them access to any services on the external network (usually the Internet). The default policy appears in the Int to Ext policy list when running in NAT mode and in the Outgoing policy list when running in Transparent mode. Default policy shows the default policy.

Default policy

Adding policies

Policies are simple to add. For example, to prevent users on the internal network connecting to FTP servers on the Internet add an Int to Ext policy that denies connections to the FTP service as shown in Sample Int to Ext policy to deny FTP connections.

Sample Int to Ext policy to deny FTP connections:

To add a policy:

Go to *Firewall > Policy* .

Click the tab corresponding to the type of policy to add.

Before adding Incoming policies in NAT mode, you must configure Virtual IP Mapping. For more information about incoming policies, see Virtual IPs.

Click New to add a policy.

You can also click Insert Policy before on a policy in the list to add the new policy above that one.

Configure the policy.

Source	Select the source address for the policy. You can only select a source address that corresponds to the type of policy that you are adding. For example, if you are adding an Int to Ext policy, you can only select an internal source address. To add addresses to this list, see Addresses.
Destination	Select the destination address for the policy. You can only select a destination address that corresponds to the type of policy that you are adding. To add addresses to this list, see Addresses.
Schedule	Select a schedule to control when to accept connections. To add schedules to this list, see Schedules.
Service	Select a service to match the type of network service controlled by the policy. For example, if the policy controls FTP connections, select FTP. By default you can select from a wide range of network services. For more information about firewall services, including how to add custom services, see Services.
Action	Select how the firewall should respond to a connection attempt matched by the policy. You can select ACCEPT to accept the connection or DENY to deny the connection. For Int to Ext policies you can also select AUTH to require users to authenticate with the firewall before the firewall accepts the connection. See Users and authentication.
Log Traffic	Optionally select Log Traffic to add messages to the traffic log whenever the policy processes a connection. See Logging and reporting.
Traffic Shaping	Optionally select Traffic Shaping to control the bandwidth available to and set the priority of the traffic processed by the policy. See Traffic shaping

Click OK to save the policy.

Sample Int to Ext (Outgoing) policy:

Editing policies

To edit a policy:

- Go to *Firewall* > *Policy* .
- Click the tab corresponding to the type of policy to edit.
- Choose a policy to edit and click Edit .
- Edit the policy settings as required.
  You can change any of the policy settings.
- Click OK to save your changes.

Policy matching

For every connection attempt, the DFL-500 must choose the policy to apply to the connection. To match a policy with a connection attempt, the DFL-500 extracts the source address, destination address, and service (or port number) from the connection attempt. Then the DFL-500 begins at the top of the policy list and searches for the first policy with matching addresses and service, and with a schedule that matches the time at which the connection attempt was received. The first policy that matches is applied to the connection attempt. If no policy matches, the connection is denied.

The default policy accepts all connection attempts from the internal network to the Internet. From the internal network, users can browse the web, use POP3 to get email, use FTP to download files through the DFL-500 and so on. If the default policy is at the top of the internal policy list, the DFL-500 allows all connections from the internal network to the Internet because all connections match with the default policy. Any policies in the list below the default policy are never matched.

For the policy to block FTP connections shown in Sample Int to Ext policy to deny FTP connections to be effective, it must be moved above the default policy in the policy list. Then, all FTP connection attempts from the internal network would match the FTP policy and be blocked. Connection attempts for all other kinds of services would not match with the FTP policy but they would match with the default policy. So the firewall would accept all other connections.

Arranging policies in the policy list

Once you have added policies to a policy list, you can use the following steps to arrange them as required.

- Go to *Firewall* > *Policy* .
- Click the tab corresponding to the policy list to arrange.
- Choose a policy to move and click Move To to change its order in the policy list.
- Type a number in the Move to field to specify where in the policy list to move the policy to and click OK.
- Click Delete to remove a policy from the list.

Controlling connections from the Internet

Use Incoming policies to give users on the Internet access to an Internet server (for example, a web server) that is protected by your firewall.

This section describes:

- Accepting incoming connections in NAT mode
- Accepting incoming connections in Transparent mode
- Denying incoming connections

Accepting incoming connections in NAT mode

Running the DFL-500 in NAT mode hides the actual addresses of the computers on your internal network from the Internet. To provide Internet access to a server on your internal network, you must add a Virtual IP that creates an association between the Internet IP address of the server and the actual address of the computer on your internal network that is running the server.

Once you have created a Virtual IP, you can add Incoming policies to accept connections to the server.

Adding an Incoming policy to accept connections

Use the following procedure to accept connections from the Internet to a server on the internal network:

- Add a Virtual IP for the server. See Adding Virtual IPs.
- Go to ***Firewall > Policy > Incoming*** .
- Click New to add a new incoming policy.
- Configure the policy (see Adding policies).

Source	Select External_All to accept connections to the server from anywhere on the Internet. You can also select an external address that limits the source addresses that the policy accepts connections from. See Addresses.
Destination	Select the Virtual IP added in Step Add a Virtual IP for the server. See "Adding Virtual IPs" .
Schedule	Select Always to accept connections at any time. To control when to accept connections add a schedule. See Schedules.
Service	Select a service to match the Internet server. For a web server, set service to HTTP. See Services.
Action	Select ACCEPT.

- Click OK to save the policy.

Accepting incoming connections in Transparent mode

In transparent mode, the addresses on the internal network are routable from the internet so you do not have to configure Virtual IP mapping. To accept connections to a server on the internal network:

- Add the address of the server to the internal address list (see Adding addresses).
- Go to ***Firewall > Policy > Incoming*** .
- Click New to add a new incoming policy.
- Configure the policy to accept connections to the internal address from the Internet for the service provided by the server (see Adding policies).

Denying incoming connections

Create policies that deny incoming connections to control access to the incoming policies that you have already created.

You can use incoming policies to deny connections:

- From addresses on the Internet (see Addresses)
- To addresses on your internal network (see Addresses)
- To services (see Services)
- According to a one-time or recurring schedule (see Schedules)

For example, you may want to periodically deny access to your public web server to allow for regular maintenance. To do this, create a recurring schedule for the maintenance period. Then create a policy that matches the original web server policy. Set the schedule of this policy to the maintenance schedule and set Action to Deny.

Since policy matching works on a first-match principle, you must add the deny policy above the accept policy in the policy list. For more information, see Policy matching and Arranging policies in the policy list.

Adding an incoming policy to deny connections

- Add the schedule for denying access. See Schedules.
- Add any addresses for which to deny connections. See Addresses.
- Go to ***Firewall > Policy > Incoming*** .
- Find the policy that you want to deny access to and click Insert Policy before .
  This inserts a new policy in the list above the policy to be denied.
- Configure the new policy to match the policy to block.
  Select the schedule that you added. Select the address you added.
  Set Action to DENY.
  For descriptions of the policy fields, see Adding policies.
- Click OK to save the policy.
  The deny policy is added to the policy list above the policy that accepts connections.

Example policy to deny access:

Controlling connections to the Internet

By default, the DFL-500 accepts all connections from the internal network to the Internet. If you do not want to enforce restrictions on access to the Internet, you do not have to change anything.

If you want to control connections to the Internet, you have three choices:

- Add exceptions to the default policy that deny connections
- Add exceptions to the default policy that require authentication
- Delete the default policy and then add policies that accept connections

In NAT mode, policies for connections from the internal network to the Internet are added to the Internal to External (Int to Ext) policies list. In Transparent mode, these policies are added to the Outgoing policies list.

This section describes:

- Denying connections to the Internet from the internal network
- Accepting connections to the Internet from the internal network
- Requiring authentication to connect to the Internet

Denying connections to the Internet from the internal network

Create policies that deny connections to the Internet from the internal network to restrict the full access to the Internet granted by the default policy.

You can use policies to deny connections:

- From addresses on your internal network (see Adding addresses)

- To addresses on the Internet (see Adding addresses)
- To services (see Services)
- According to a one-time or recurring schedule (see Schedules)

Since policy matching works on a first-match principle, you must add deny policies above the default policy. You must also add deny policies above matching policies that accept connections. For more information, see Policy matching and Arranging policies in the policy list.

Adding a policy to deny connections

- Add addresses, services, or schedules as required.
- Go to ***Firewall > Policy > Int to Ext*** . In Transparent mode go to ***Firewall > Policy > Outgoing*** .
- Click New to add a policy.

  You can also click Insert Policy before on a policy in the list to add the new policy above a specific policy.
- Configure the policy to match the connection to block and set Action to DENY.

  For descriptions of the policy fields, see Adding policies.
- Click OK to save the policy.

Policy to deny FTP connections to the Internet from an internal subnet:

Accepting connections to the Internet from the internal network

Create policies that accept connections to the Internet from the internal network to control the connections that are available.

You can use policies to accept connections:

- From addresses on your internal network (see Adding addresses)
- To addresses on the Internet (see Adding addresses)
- To services (see Services)
- According to a one-time or recurring schedule (see Schedules)

Policies that accept connections can be used in the following ways:

- Add policies that accept connections as exceptions to policies that deny connections

For example, if a policy denies connections to a subnet, you can add a policy that accepts connections from one of the computers on the subnet. Policies that accept connections in this way must be added to the policy list above the connections that they are exceptions to.

- Delete the default policy and then add policies to accept only the connections that you want the firewall to accept

  In this way you can limit Internet access to that allowed in the policies that you create. You must delete the default policy because if it remains in the policy list, all connections that do not match another policy will be accepted by the default policy.

Adding a policy to accept connections

- Add addresses, services, or schedules as required.
- Go to ***Firewall > Policy > Int to Ext*** . In Transparent mode go to ***Firewall > Policy > Outgoing*** .
- Click New to add a policy.

  You can also click Insert Policy before on a policy in the list to add the new policy above a specific policy.
- Configure the policy to match the type of connection to accept.

  Set Action to ACCEPT.
  For descriptions of the policy fields, see Adding policies.
- Click OK to save the policy.

Requiring authentication to connect to the Internet

When running the DFL-500 in NAT mode, you can configure policies to require users on the internal network to enter a user name and password to access the Internet. To require authentication you must add users to the firewall configuration, see Adding user names and passwords.

You can add policies to require user authentication for connections:

- From addresses on your internal network (see Adding addresses)
- To addresses on the Internet (see Adding addresses)
- Using certain services (see Services)
- During a one-time or recurring schedule (see Schedules)

Since policy matching works on a first-match principle, you must add authentication policies above the default policy. You must also add authentication policies above matching policies that accept or deny connections. For more information, see Policy matching and Arranging policies in the policy list.

Adding a policy to require authentication

Use the following procedure to require users to authenticate before being able to access the internet:

- Add user names and passwords to the firewall. See Users and authentication.
- Go to ***Firewall > Policy > Int to Ext*** .
- Click New to add a policy.
- Configure the policy to match the type of connection for which to require authentication.

  Set Action to AUTH.
  For descriptions of the policy fields, see Adding policies.
- Click OK to save the policy.

Addresses

All DFL-500 policies require source and destination IP addresses. By default the DFL-500 includes two addresses that cannot be edited or deleted:

- Internal_All on the Internal address list which represents the IP addresses of all of the computers on your internal network
- External_All on the External address list which represents the IP addresses of all of the computers on the Internet

You can add the following types of addresses:

- Internal addresses define addresses on your internal network

  In NAT mode, Internal addresses can be the source address of an Int to Ext policy. In Transparent mode, internal addresses can be the source address of an Outgoing policy and the destination address of an Incoming policy.
- External addresses define addresses on the Internet

  In NAT mode, external addresses can be added to the source address of an Incoming policy and the destination addresses of an Int to Ext policy.
  In Transparent mode, external addresses can be the source address of an Incoming policy and the destination addresses of an Outgoing policy.

This section describes:

- Adding addresses
- Editing addresses

Adding addresses

- Go to *Firewall* > *Address* .

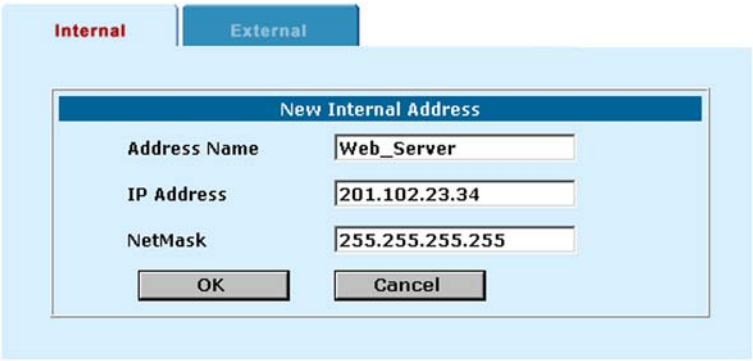
  Click the tab corresponding to the type of address you want to add.
- Click New to add a new address.
- Enter an Address Name to identify the address.

  The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and the @ character are not allowed.
- Add the IP Address.

  The IP Address can be the IP address of a single computer (for example, 192.45.46.45) or the address of a subnetwork (for example, 192.168.1.0).
- Add the NetMask.

  The Netmask should correspond to the address. The Netmask for the IP address of a single computer should be 255.255.255.255, The Netmask for a subnet should be 255.255.255.0.
- Click OK to add the address.

Example internal address:



Editing addresses

- Go to *Firewall* > *Address* .
  Click the tab corresponding to the type of address you want to edit.
- Choose an address to edit and click Edit .
- Make the required changes and click OK to save your changes.

Services

Use services to control the types of communication accepted or denied by the firewall. You can add any of the pre-configured services listed in DFL-500 pre-defined services to a policy. You can also create your own custom services and add services to service groups.

This section describes:

- Pre-defined services
- Providing access to custom services
- Grouping services

Pre-defined services

The DFL-500 pre-defined services are listed in DFL-500 pre-defined services.

DFL-500 pre-defined services

Service name	Description	Protocol	Source Port	Destination port
ANY	Match connections on any port.	all	1-65535	all
DNS	Domain name servers for looking up domain names.	tcp	1-65535	53
		udp	1-65535	53
FINGER	Finger service.	tcp	1-65535	79
FTP	FTP service for transferring files.	tcp	1-65535	20-21
GOPHER	Gopher communication service.	tcp	1-65535	70
HTTP	HTTP service for connecting to web pages.	tcp	1-65535	80
HTTPS	SSL service for secure communications with web servers.	tcp	1-65535	443

IMAP	IMAP email protocol for reading email from an IMAP server.	tcp	1-65535	143
IRC	Internet relay chat for connecting to chat groups.	tcp	1-65535	6660-6669
NFS	Network file services for sharing files.	tcp	1-65535	111
				2049
		udp	1-65535	111
				2049
NNTP	Protocol for transmitting Usenet news.	tcp	1-65535	119
NTP	Network time protocol for synchronizing a computer's time with a time server.	tcp	1-65535	123
		udp	1-65535	123
PING	For testing connections to other computers.	icmp	1-65535	0
				8
POP3	POP3 email protocol for downloading email from a POP3 server.	tcp	1-65535	110
		udp	1-65535	110
QUAKE	For connections used by the popular Quake multi-player computer game.	udp	1-65535	26000
				27000
				27910
				27960
RAUDIO	For streaming real audio multi-media traffic.	udp	1-65535	7070
RLOGIN	Rlogin service for remotely logging into a server.	tcp	1-65535	513
SMTP	For sending mail between email servers on the Internet.	tcp	1-65535	25
SNMP	For communicating system status information.	tcp	1-65535	161-162
		udp	1-65535	161-162
SSH	SSH service for secure connections to computers for remote management.	tcp	1-65535	22
		udp	1-65535	22
TELNET	Telnet service for connecting to a remote computer to run commands.	tcp	1-65535	23
VDOLIVE	For VDO Live streaming multimedia traffic.	udp	1-65535	7000
WAIS	Wide Area Information Server. An Internet search protocol.	tcp	1-65535	210
X-WINDOWS	For remote communications between an X-Window server and X-Window clients.	tcp	1-65535	6000

Providing access to custom services

Add a custom service if you need to create a policy for a service that is not in the predefined services list. Use the following procedure to add your own custom service.

- Go to *Firewall* > *Service* > *Custom* .
- Click New.
- Enter a Name for the service. This name appears in the service list used when you add a policy.

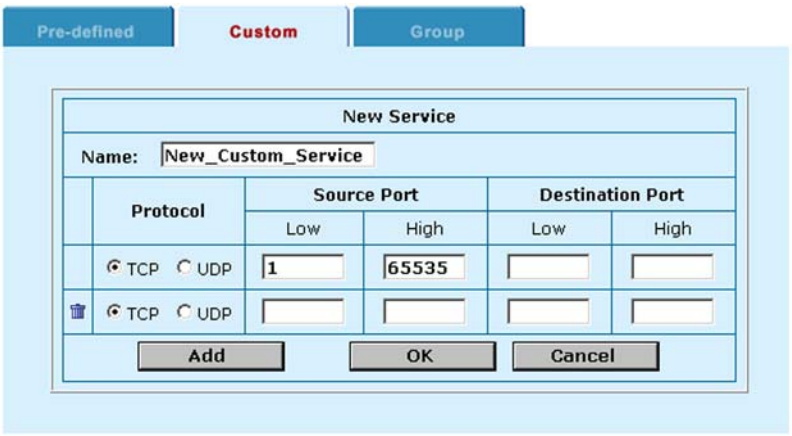
  The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and the @ character are not allowed.
- Select the protocol (either TCP or UDP) used by the service.

- Specify a port number range for the service by adding the low and high port numbers. If the service uses one port number, add this number to both the Low and High fields.
- If the service has more than one port range, click Add to specify additional protocols and port ranges.

  If you mistakenly add too many port range rows, click delete to remove the extra row.
- Click OK to add the custom service.

  You can now add this custom service to a policy (see Policies).

Adding a custom service:



Grouping services

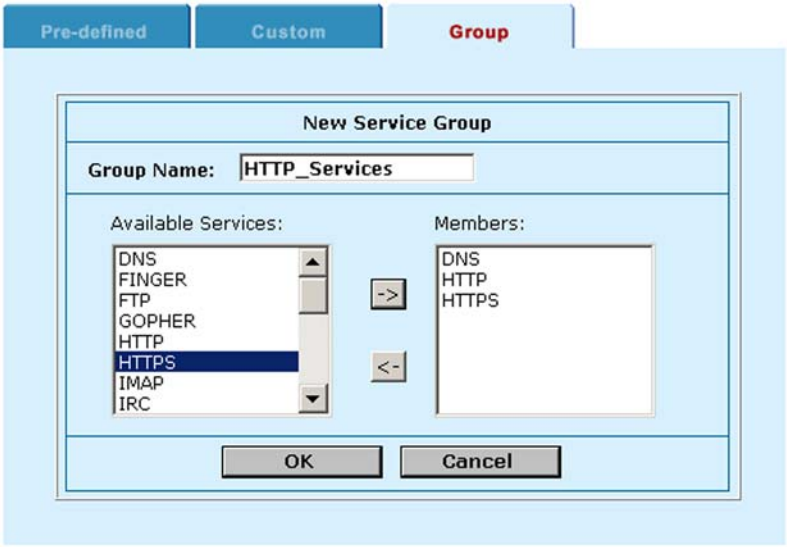
To make it easier to add policies, you can create groups of services and then add one policy to provide access to or block access for all the services in the group. A service group can contain pre-defined services and custom services in any combination. You cannot add service groups to another service group.

To add a service group:

- Go to *Firewall* > *Service* > *Group* .
- Click New.
- Enter a Group Name to identify the group. This name appears in the service list used when you add a policy.

  The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and the @ character are not allowed.
- To add services to the service group, select a service from the Available Services list and click the right arrow to copy it to the Members list.
- To remove services from the service group, select a service from the Members list and click the left arrow to remove it from the group.
- Click OK to add the service group.

Adding a service group:



Schedules

Use scheduling to control when policies are active or inactive. You can create one-time schedules and recurring schedules. You can use one-time schedules to create policies that are effective once only for the period of time specified in the schedule. Recurring schedules repeat weekly. You can use recurring schedules to create policies that are effective only at specified times of the day or on specified days of the week.

In some cases, you may be required to create multiple schedules to schedule a policy to be active for more than a single day. For example, for a policy to be valid from Monday at 5:00 pm until Tuesday at 9:00 am, you must create two schedules and then two policies, one for each schedule. The first schedule should run from Monday evening at 5:00 pm until midnight and the second from midnight until 9:00 am on Tuesday morning.

This section describes:

- Creating one-time schedules
- Creating recurring schedules
- Applying a schedule to a policy

Creating one-time schedules

You can create a one-time schedule that activates or deactivates a policy for a specified period of time. For instance, your firewall may be configured with the default Internal to External policy that allows access to all services on the Internet at all times. You can add a one-time schedule to block access to the Internet during a holiday period. The following procedure describes how to create a one-time schedule with a start date at the start of the holiday and an end date at the end of the holiday.

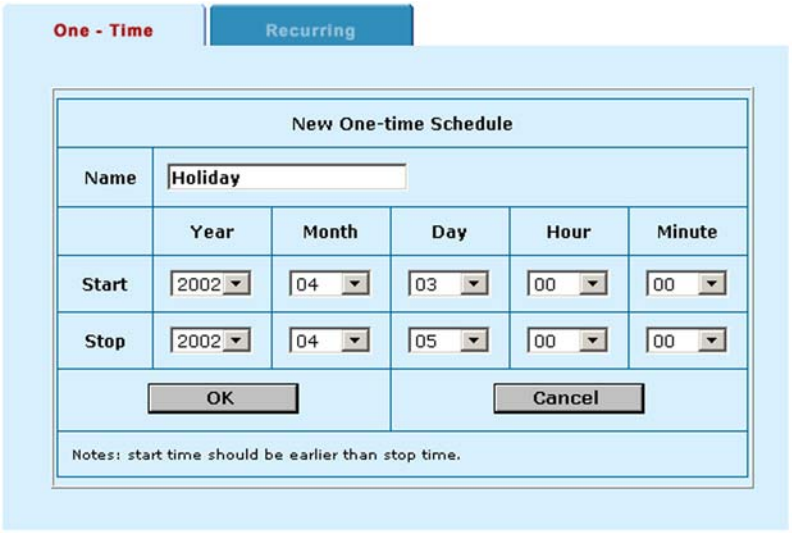
- Go to *Firewall* > *Schedule* > *One-time* .
- Click New.
- Specify a name for the schedule.

  The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and the @ character are not allowed.
- Specify the Start date and time for the schedule.

  Set start and stop times to 00 for the schedule to cover the entire day.

- Specify the Stop date and time for the schedule.
  One-time schedules use the 24-hour clock.
- Click OK to add the One-time schedule.

Sample one-time schedule:



Creating recurring schedules

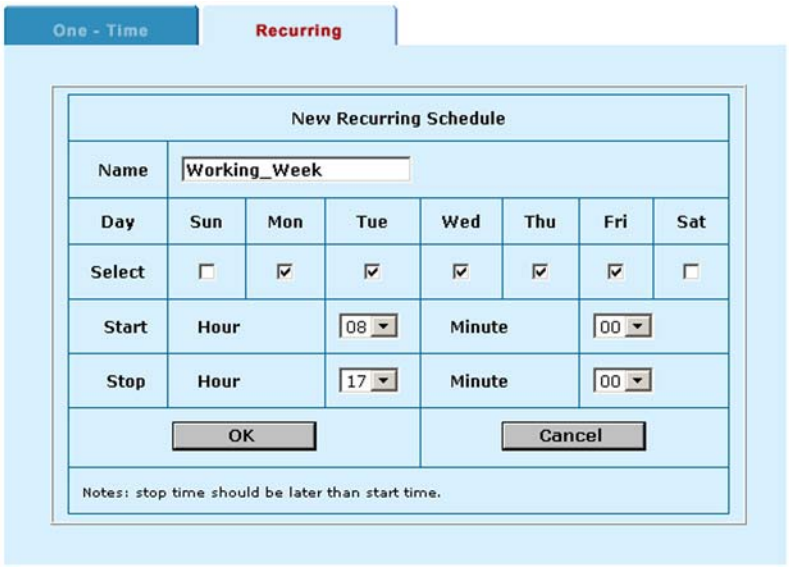
You can create a recurring schedule that activates or deactivates policies at specified times of the day or on specified days of the week. For instance, you may wish to prevent internet use outside of working hours by creating a recurring schedule.

- Go to ***Firewall > Schedule > Recurring*** .
- Click New to create a new schedule.
- Specify a name for the schedule.
  The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and the @ character are not allowed.
- Select the days of the week that are working days.
- Set the Start Hour and the End Hour to the start and end of the work day.

  The Recurring schedule uses a 24-hour clock.

- Click OK.

Sample recurring schedule:



Applying a schedule to a policy

Once you have created schedules you can add them to policies to schedule when the policies are active.

- Go to *Firewall* > *Policy* .
- Click the tab corresponding to the type of policy to add.
- Click New to add a policy.
- Configure the policy as required.
- Add a schedule by selecting it from the Schedule list.
- Click OK to save the policy
- Arrange the policy in the policy list to have the effect that you expect.

  For example, to use a one-time schedule to deny access to another policy, add a policy that matches the other policy in every way. Choose the one-time schedule that you added and set Action to Deny. Then you must arrange the policy containing the one-time schedule in the policy list above the policy to be denied.

Arranging a one-time schedule in the policy list to deny access.

Users and authentication

You can configure the DFL-500 to require users to authenticate (enter a user name and password) to access services through the firewall. To configure authentication you need to add user names and passwords to the firewall and then add policies that require authentication. When a connection attempt is matched by a policy requiring authentication, the user requesting the connection must enter a valid user name and password to be allowed to connect through the firewall.

Requiring passwords is not supported in Transparent mode.

You can add authentication to Int to Ext policies, but not to Incoming policies.

Users can only enter passwords using HTTP, FTP, or Telnet. If users are required to enter a user name and password to access the Internet, they must connect to the firewall using a web browser, FTP, or Telnet to enter their user name and password.

Use the following procedures for:

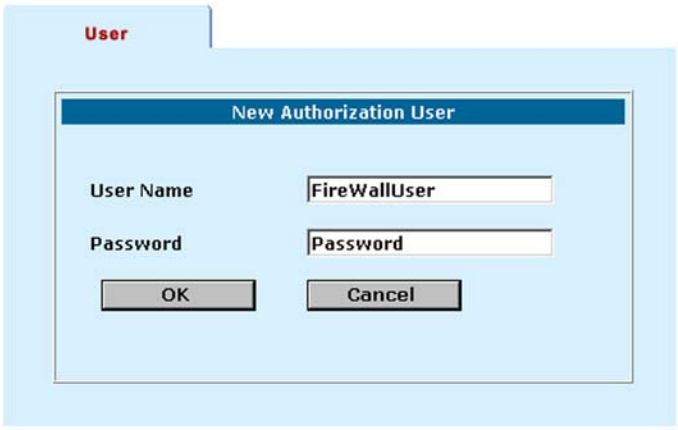
- Adding user names and passwords
- Setting authentication time out
- Adding authentication to a policy

Adding user names and passwords

- Go to *Firewall* > *Users* .
- Click New.
- Enter a User Name and Password.

  The user name and the password must be at least 6 characters long and can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and the @ character are not allowed.
- Click OK.

Adding a user name and password:



Setting authentication time out

To set authentication time out:

- Go to *System* > *Config* > *Options* .
- Set Auth Timeout to control how long authenticated connections can remain idle before users have to authenticate again to get access through the firewall.

The default authentication time out is 5 minutes.

Adding authentication to a policy

Once you have added user names and passwords you can add or edit policies to require authentication.

- Go to *Firewall* > *Policy* .

- Click the tab corresponding to the type of policy to add.
- You can add authentication to Int to Ext policies.
- Click New to add a policy or click Edit to edit a policy to add authentication.
- Configure the policy as required.
- Set Action to Auth.
- Click OK to save the policy
- Arrange the policy in the policy list to have the effect that you expect.

Polices that require authentication must be added to the policy list above matching policies that do not, otherwise the policy that does not require authentication is selected first.

Virtual IPs

Running the DFL-500 in NAT mode hides the addresses of the computers on your internal network from the Internet. To provide Internet access to a server on your internal network, you must make an association between the Internet address of the server and the actual IP address of the computer on the internal network that is running the server. This association is called a Virtual IP.

Once you have created a Virtual IP, you can add Incoming policies to allow access to the server by adding the virtual IP to the Destination address of the policy.

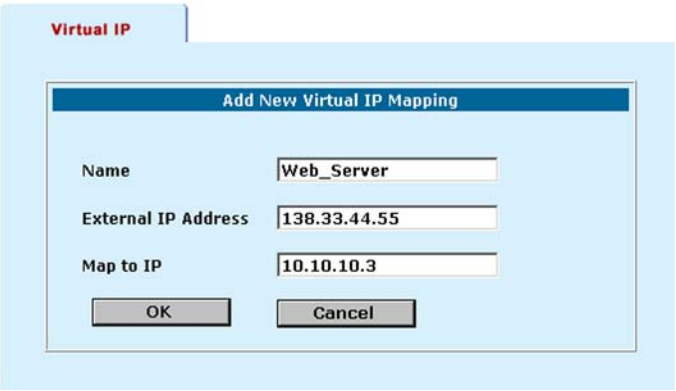
Adding Virtual IPs

- To add a Virtual IP:
- Go to *Firewall* > *Virtual IP* .
- Click New to add the Virtual IP.
- Enter a Name for the Virtual IP.

  The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and the @ character are not allowed.
- In the External IP Address field, enter the Internet IP address of the server.

  This must be a static IP address obtained from your ISP for this purpose and must not be the same as the external address of the DFL-500. However, your ISP must route this address to the external IP address of the DFL-500.
- In the Map to IP field, enter the actual IP address of the web server.
- Click OK to save the Virtual IP.
- Repeat these steps to add Virtual IPs for all of your internet servers.

Adding a Virtual IP:



IP/MAC binding

IP/MAC binding provides added security against IP Spoofing attacks. IP Spoofing attempts to use the IP address of a trusted computer to access the DFL-500 from a different computer. The IP address of a computer can easily be changed to a trusted address, but MAC addresses are added to ethernet cards at the factory and cannot easily be changed.

You can enter the IP addresses and corresponding MAC addresses of trusted computers into the DFL-500 firewall configuration. When a data packet arrives from a trusted IP address, it is checked to determine whether the MAC address that the packet originated from matches the MAC address in the table. The DFL-500 checks all packets arriving at the DFL-500 whether they are directed at the DFL-500 or are meant to be passed through.

MAC addresses are only carried on the local network where they originate, and are not passed from one network to another.

This section describes:

- Adding IP/MAC binding addresses
- Enabling IP/MAC binding

Adding IP/MAC binding addresses

- Go to *Firewall* > *IP/MAC Binding* > *IP MAC* .
- Click New to add an IP address/MAC address pair.
- Click Enable to activate the IP/MAC binding pair.

Enabling IP/MAC binding

- Go to *Firewall* > *IP/MAC Binding* > *Setting* .
- Click Enable IP/MAC.
- Select one of the following:

Allow traffic when not defined in the table	The DFL-500 lets traffic with a source address not found in the IP/MAC binding table pass through the firewall. Any traffic with a source address that is defined in the IP/MAC binding table must have the correct MAC address or it is blocked.
Deny traffic when not defined in the table	The DFL-500 blocks all traffic with a source address that is not found in the IP/MAC binding table. Any traffic with a source address that is defined in the IP/MAC binding table must have the correct MAC address or it is also blocked.

- Click Apply to save your changes.

Traffic shaping

You can use traffic shaping to guarantee the amount of bandwidth available through the firewall for a policy. Guarantee bandwidth to make sure that there is enough bandwidth available for a hi-priority service.

You can also use traffic shaping to limit the amount of bandwidth available through the firewall for a policy. Limit bandwidth to keep less important services from using bandwidth needed for more important services.

Adding traffic shaping to a policy

You can add traffic shaping to any type of policy. The following procedure describes adding traffic shaping to an Int to Ext policy.

- Go to *Firewall* > *Policy* > *Int to Ext* .
- Choose a policy to add traffic shaping to and click Edit .
- Turn on traffic shaping.
- Configure traffic shaping for the policy:

Guaranteed bandwidth	Available in a future release.
Maximum bandwidth	Available in a future release.
Traffic Priority	Select high, medium, or low.

- Click OK to save your changes to the policy.

IPSec VPNs

Using DFL-500 IPSec Virtual Private Networking (VPN), you can join two or more widely separated private networks together through the Internet. For example, a company that has two offices in different cities, each with its own private network, can use VPN to create a secure tunnel between the offices. In addition, remote or travelling workers can use a VPN client to create a secure tunnel between their computer and their office private network.

The secure IPSec VPN tunnel makes it appear to all computer users that they are on physically connected networks. The VPN protects data passing through the tunnel by encrypting it to guarantee confidentiality. In addition, authentication guarantees that the data originated from the claimed sender and was not damaged or altered in transit.

IPSec is an internet security standard for VPN and supported by most VPN products. DFL-500 IPSec VPNs can be configured to use Autokey Internet Key Exchange (IKE) or manual key exchange. Autokey key exchange is easier to configure and maintain than manual key exchange. However, manual key exchange is available for compatibility with third party VPN products that require it.

IPSec VPN is only supported in NAT mode.

This chapter describes:

- Compatibility with third-party VPN products
- Autokey IPSec VPN between two networks
- Autokey IPSec VPN for remote clients
- Manual key exchange IPSec VPN between two networks
- Manual key exchange IPSec VPN for remote clients
- Testing a VPN
- IPSec VPN pass through

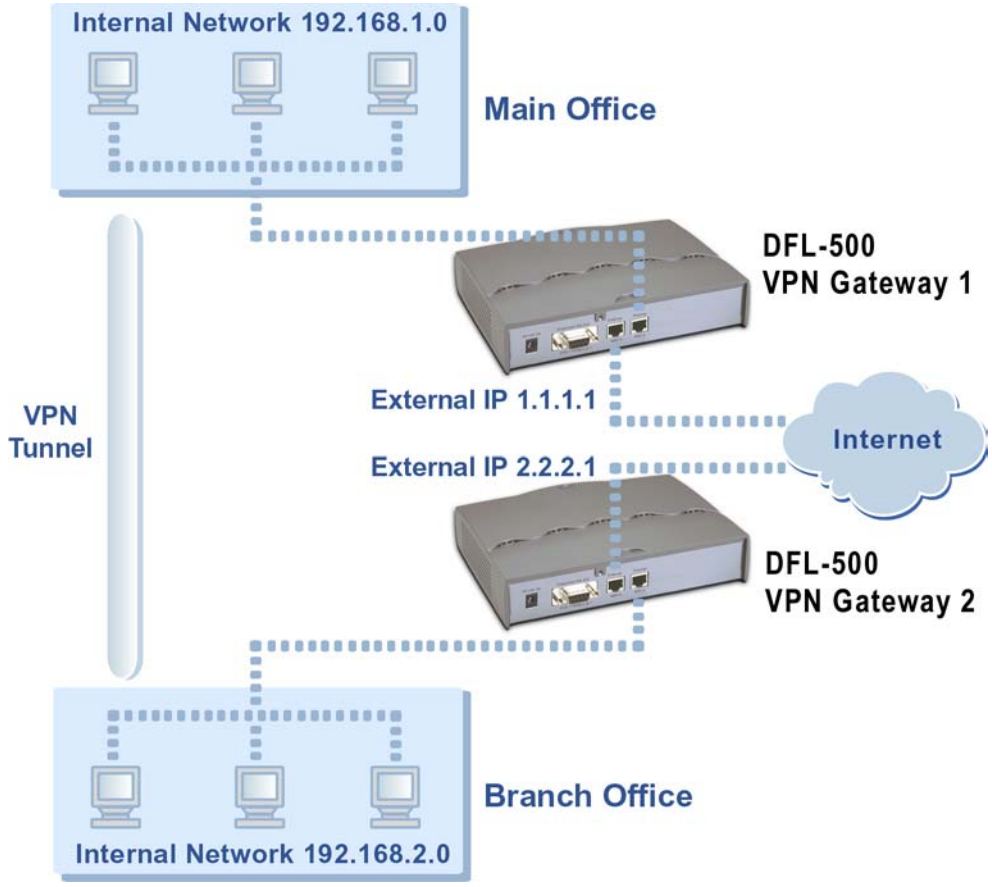
Compatibility with third-party VPN products

Because the DFL-500 supports the IPSec industry standard for VPN, you can configure a VPN between the DFL-500 and any third party VPN client or gateway/firewall that supports IPSec VPN. To successfully establish the tunnel, the VPN settings must be the same on the DFL-500 and the third party product.

DFL-500 IPSec VPNs support:

- IPSec Internet Protocol Security standard
- Automatic IKE based on Pre-shared Key
- Fully customizable manual keys
- ESP security in tunnel mode
- 3DES (TripleDES) encryption
- HMAC MD5 authentication/data integrity or HMAC SHA authentication/data integrity

Example VPN between two internal networks:



Autokey IPSec VPN between two networks

Use the following procedures to configure a VPN that provides a direct communication link between users and computers on two different networks. Example VPN between two internal networks shows an example VPN between the main office and a branch office of a company. Users on the main office internal network can connect to the branch office internal network and users on the branch office internal network can connect to the main office internal network. Users on the branch office network can also connect to services such as an email server running on the main network.

Communication between the two networks takes place in an encrypted VPN tunnel that connects the two DFL-500 VPN gateways across the Internet. Users on the internal networks are not aware that when they connect to a computer on the other network that the connection is across the Internet.

As shown in Example VPN between two internal networks, each internal network can be protected by a DFL-500 VPN gateway. Alternatively, one of the networks can be protected by a third-party VPN gateway that also supports IPSec and Autokey IKE.

Use the following procedures to configure an IPSec Autokey IKE VPN between internal networks:

- Creating the VPN tunnel
- Adding internal and external addresses
- Adding an IPSec VPN policy

Creating the VPN tunnel

A VPN tunnel consists of a name for the tunnel, the IP address of the VPN gateway at the opposite end of the tunnel, the keylife for the tunnel, and the authentication key to be used to start the tunnel. You must create complementary VPN tunnels on each of the VPN gateways. On both gateways the tunnel should have the same name, keylife, and authentication key.

Example IPSec Autokey VPN Tunnel configuration shows the information required to configure the VPN tunnel for the VPN in Example VPN between two internal networks.

Example IPSec Autokey VPN Tunnel configuration

	Description	Main Office	Branch Office
VPN Tunnel Name	Use the same name on both ends of the tunnel. The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and the @ character are not allowed.	Branch_Office_VPN	Branch_Office_VPN
Remote Gateway	The External IP address of the VPN gateway at the other end of the VPN tunnel.	2.2.2.1	1.1.1.1
Keylife	The amount of time (5 to 1440 minutes) before the encryption key expires. When the key expires, the VPN gateways generate a new key without interrupting service.	100	100
P1 Proposal	Select the Encryption and algorithm to propose for Phase 1 of the IPSec VPN connection.	DES and 3DES	DES and 3DES
	Select the Authentication algorithms to propose for Phase 1 of the IPSec VPN connection.	MD5	MD5
P2 Proposal	Select the algorithms to propose for Phase 2 of the IPSec VPN connection.		
Authentication Key	Enter up to 20 characters. The key must be the same on both VPN gateways and should only be known by network administrators.	ddcHH01887d	ddcHH01887d

About P1 and P2 proposals

IPSec VPNs use a two-phase process for creating a VPN tunnel. During the first phase (P1) the VPN gateways at each end of the tunnel negotiate to select a common algorithm for encryption and another one for authentication. When you select a P1 Proposal, you are selecting the algorithms that the DFL-500 proposes during Phase 1 negotiation. You can choose two encryption and two authentication algorithms. Usually you would choose both, to make it easier for P1 negotiation. But you can restrict the choice to one if required. For negotiation to be successful, each VPN gateway should have at least one encryption algorithm and one authentication algorithm in common.

During the second phase (P2) the VPN gateways negotiate to select a common algorithm for data communication. When you select algorithms for the P2 Proposal, you are selecting the algorithms that the DFL-500 will propose during Phase 2 negotiation. Again, during P2, each VPN gateway should have at least one algorithm in common.

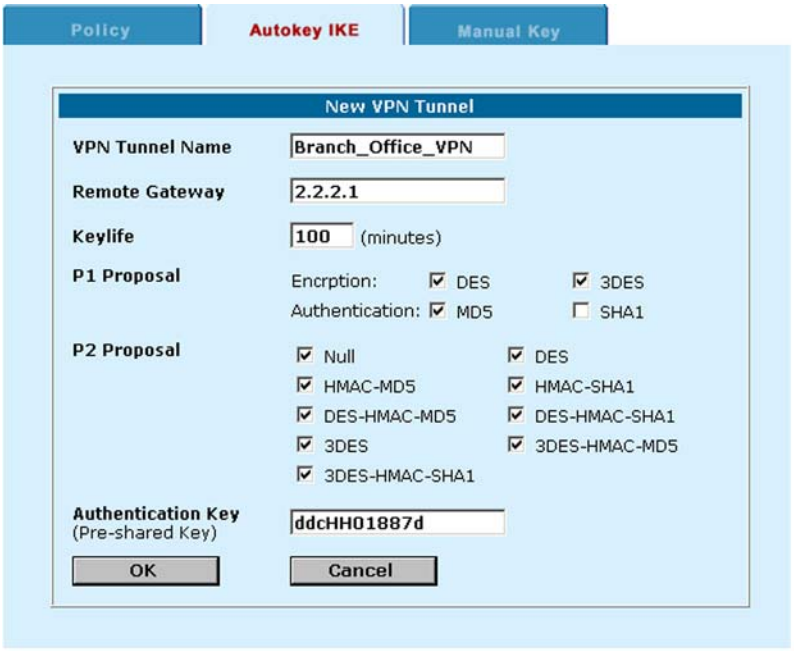
Creating the VPN tunnel

Complete the following procedure on both VPN gateways to configure a VPN tunnel that uses Autokey IKE key exchange:

- Go to *VPN* > *IPSEC* > *Autokey IKE* .
- Click New to add a new Autokey IKE VPN tunnel.
- Enter the VPN Tunnel Name, Remote Gateway, Keylife and Authentication Key.
- Select the P1 Proposal and P2 Proposal algorithms.

- Click OK to save the Autokey IKE VPN tunnel.

Example Main Office Autokey IKE VPN tunnel:



Adding internal and external addresses

The next step in configuring the VPN is to add the addresses of the networks that are to be connected using the VPN tunnel. On each VPN gateway you must add two addresses:

- Internal address, the IP address of the network behind the VPN gateway
- External address, the IP address of the network behind the other VPN gateway

IPSec Autokey VPN addresses shows the internal and external addresses required for the VPN in Example VPN between two internal networks. In the example, both IP addresses are for internal networks.

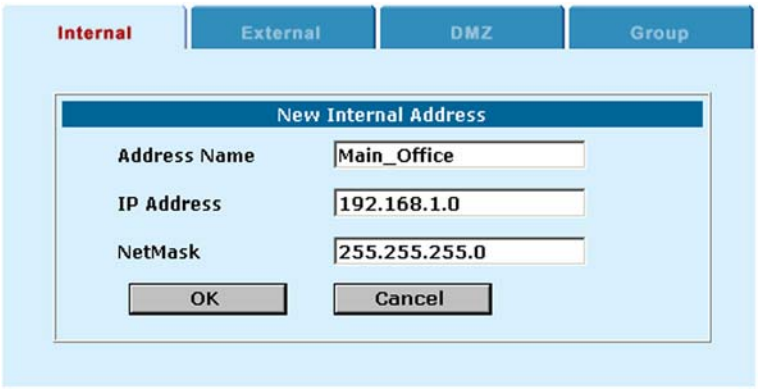
IPSec Autokey VPN addresses

	Description	Main Office	Branch Office
Internal Address			
Address Name	The name to assign to the internal network to be connected using the VPN. The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and the @ character are not allowed.	Main_Office	Branch_Office
IP address	The IP address and netmask of the internal network.	192.168.1.0	192.168.2.0
Netmask		255.255.255.0	255.255.255.0
External Address			
Address Name	The name to assign to the internal network to be connected to the opposite end of the VPN tunnel.	Branch_Office	Main_Office
IP address	The IP address and netmask of the internal network at the other end of the VPN tunnel.	192.168.2.0	192.168.1.0
Netmask		255.255.255.0	255.255.255.0

Complete the following procedure on both VPN gateways to add the internal and external IP addresses:

- Go to *Firewall* > *Address* > *Internal* .
- Click New to add a new internal address.
- Enter the Address Name and the IP Address and NetMask of the internal network that can connect to the VPN.

Example internal address for VPN Gateway 1:



- Click OK to save the internal address.
- Go to ***Firewall > Address > External*** .
- Click New to add a new external address.
- Enter the Address Name and the IP Address and NetMask of the network behind the other VPN gateway.
- Click OK to save the external address.

Adding an IPSec VPN policy

The VPN policy associates the source and destination addresses created in the previous procedure with the VPN tunnel created in the first procedure. Each VPN gateway then receives all traffic from the internal address that is destined for the external address and routes it across the Internet to the other VPN gateway using the VPN tunnel.

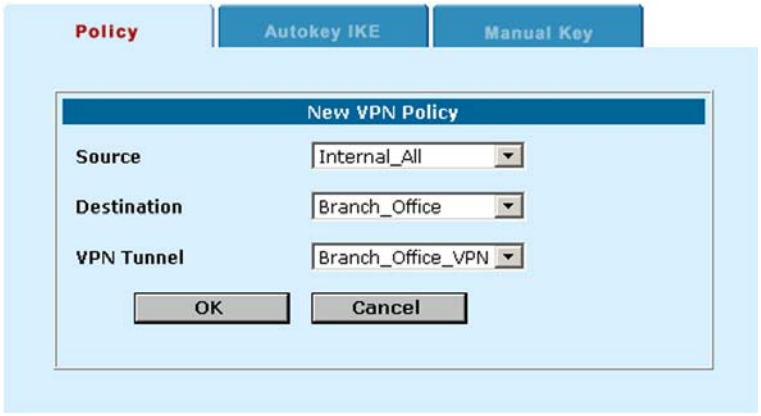
Example IPSec Autokey VPN policy configuration

	Description	**Main Office (VPN Gateway 1)**	**Branch Office (VPN Gateway 2)**
Source IP address	The Internal IP address (See IPSec Autokey VPN addresses).	Main_Office	Branch_Office
Destination IP Address	The External IP address (See IPSec Autokey VPN addresses).	Branch_Office	Main_Office
VPN Tunnel Name	The name of the VPN tunnel (See Example IPSec Autokey VPN Tunnel configuration).	Branch_Office_VPN	Branch_Office_VPN

Complete the following procedure on both VPN gateways to add the VPN policy:

- Go to *VPN* > *IPSEC* > *Policy* .
- Click New to add a new IPSec VPN policy.
- Configure the VPN Policy.
- Click OK to save the VPN policy.

Example Main Office VPN policy:



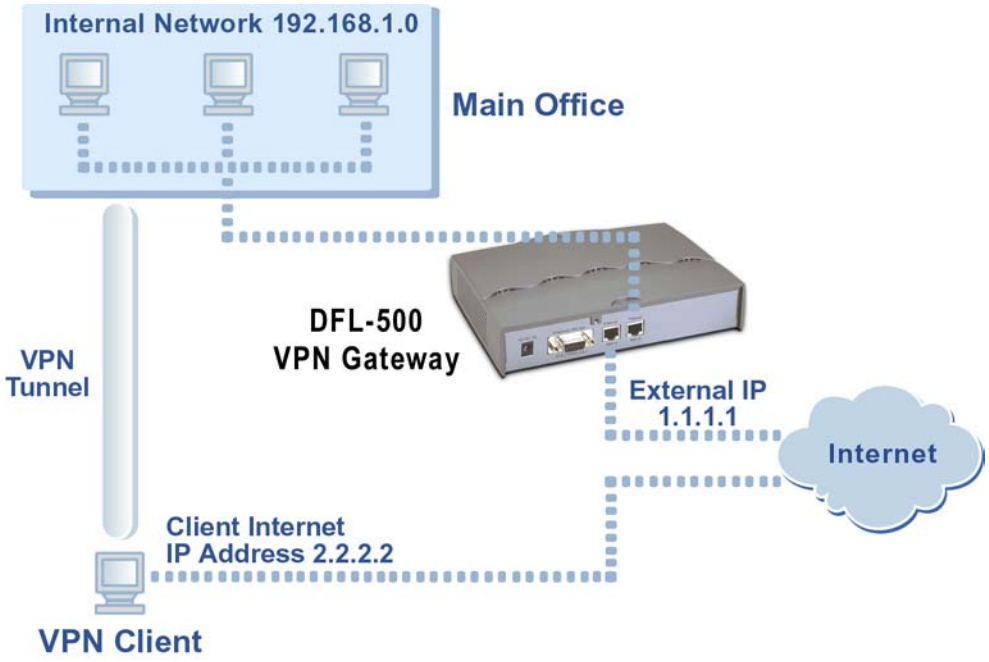
Autokey IPSec VPN for remote clients

Use the following procedures to configure a VPN that allows remote VPN clients to connect to users and computers on a Main Office internal network (See Example VPN between an internal network and remote clients). A remote VPN client can be any computer connected to the Internet and running VPN client software that uses IPSec and Autokey IKE. The client can have a static IP address or a dynamic IP address. A remote client could be:

- A traveller using a dial-up connection to connect to the Internet
- A telecommuter using an ISP to connect to the Internet from home

Communication between the remote users and the internal network takes place over an encrypted VPN tunnel that connects the remote user to the DFL-500 VPN gateway across the Internet. Once connected to the VPN, the remote user's computer appears as if it is installed on the internal network.

Example VPN between an internal network and remote clients:



Use the following procedures to configure an IPSec Autokey IKE VPN that allows VPN clients to connect to an internal network:

- Configuring the VPN tunnel for the client VPN
- Adding internal and external addresses
- Adding an IPSec VPN policy
- Configuring the IPSec VPN client

Configuring the VPN tunnel for the client VPN

A VPN tunnel consists of a name for the tunnel, the remote gateway IP address (which is the IP address of the client), the keylife for the tunnel, and the authentication key to be used to start the tunnel.

You can either create multiple VPN tunnels, one for each VPN client, or you can create one VPN tunnel with a remote gateway address set to 0.0.0.0. This VPN tunnel accepts connections from any Internet address.

You must create complementary VPN tunnels on the VPN gateway and the clients. On both, the tunnel must have the same name, keylife, and authentication key.

Example VPN Tunnel configuration shows the information required to configure the VPN tunnel for the VPN in Example VPN between an internal network and remote clients.

Example VPN Tunnel configuration

	Description	Example Setting
VPN Tunnel Name	Use the same name on both ends of the tunnel. The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and the @ character are not allowed.	Client_VPN
Remote Gateway	To accept connections from a client at a static IP address (for example, 2.2.2.2).	2.2.2.2
	To accept connections from any Internet address (for a client with a dynamic IP address).	0.0.0.0
Keylife	The amount of time (5 to 1440 minutes) before the encryption key expires. When the key expires, the VPN gateway and the client generate a new key without interrupting service.	100
P1 Proposal	Select the Encryption algorithms to propose for Phase 1 of the IPSec VPN connection.	DES and 3DES
	Select the Authentication algorithms to propose for Phase 1 of the IPSec VPN connection.	MD5
P2 Proposal	Select the algorithms to propose for Phase 2 of the IPSec VPN connection. For more information, see See About P1 and P2 proposals.	
Authentication Key	Enter up to 20 characters. The VPN gateway and clients must have the same key and it should only be known by network administrators.	ddcHH01887d

Complete the following procedure on the DFL-500 VPN gateway.

- Go to *VPN* > *IPSEC* > *Autokey IKE* .
- Click New to add a new Autokey IKE VPN tunnel.
- Enter the VPN Tunnel Name, Remote Gateway, Keylife, and Authentication Key.
- Select the P1 Proposal and the P2 Proposal algorithms.
- Click OK to save the Autokey IKE VPN tunnel.

Adding internal and external addresses

The next step in configuring the VPN is to add the addresses of the VPN clients and the address of the internal network to the VPN gateway.

You do not have to add addresses for remote clients with dynamic IP addresses.

Example VPN Gateway IP Addresses shows the internal and external addresses required for the VPN Gateway shown in Example VPN between an internal network and remote clients.

Example VPN Gateway IP Addresses		
	Description	**Example Setting**
Internal Address		
Address Name	The name to assign to the internal network that the VPN client can connect to. The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and the @ character are not allowed.	Main_Office
IP address	The IP address and netmask of the internal network that the VPN client can connect to.	192.168.1.0
Netmask		255.255.255.0
External Address		
Address Name	The name to assign to the VPN client.	VPN_Client
IP address	The IP address and netmask of a VPN client with a static IP address (for example, 2.2.2.2). You do not have to add an address for a client with a dynamic IP address.	2.2.2.2
Netmask		255.255.255.255

Complete the following procedure on the VPN gateway to add the internal and client IP addresses:

- Go to *Firewall* > *Address* > *Internal* .
- Click New to add a new internal address.
- Enter an Address Name, IP Address and NetMask for the internal network.
- Click OK to save the internal address.
- Go to ***Firewall > Address > External*** .
- Click New to add the static IP address of the client.
- Enter an Address Name, IP Address, and NetMask for the VPN client.
- Click OK to save the client address.

Adding an IPSec VPN policy

The VPN policy associates the source address of the internal network and the destination address of the VPN client with the VPN tunnel created for the VPN client. The VPN gateway then starts up the VPN tunnel whenever it receives packets from the VPN client. Once the VPN tunnel is established, all traffic between the VPN client and the VPN gateway that is destined for the internal network is routed across the Internet in the VPN tunnel.

Example VPN Gateway policy configuration		
	Description	**Example setting**
Source IP address	The Internal IP address (See Example VPN Gateway IP Addresses).	Main_Office
Destination IP	The Internet IP address of the client (See Example VPN Gateway IP Addresses).	VPN_Client

Address		
VPN Tunnel Name	The name of the VPN tunnel to be created between the VPN gateway and the VPN client (See Example VPN Tunnel configuration).	Client_VPN

Complete the following procedure on the VPN gateway to add the VPN policy:

- Go to *VPN* > *IPSEC* > *Policy* .
- Click New to add a new IPSec VPN policy.
- Select the Source IP address, Destination IP address, and the VPN tunnel to add to the IPSec VPN policy.
- Click OK to save the VPN policy.

Configuring the IPSec VPN client

The VPN client PC must be running industry standard IPSec Autokey IKE VPN client software. D-Link recommends the SafeNet/Soft-PK client from IRE, Inc.

Configure the client as required to connect to the VPN gateway using an IPSec VPN configuration. Make sure the client configuration includes the settings in VPN client configuration. These settings should match the VPN Gateway configuration.

VPN client configuration

	Description	**Example Setting**
VPN Tunnel Name	Should correspond to the VPN tunnel name used on the VPN gateway.	Client_VPN
Remote Gateway	The External IP address of the VPN gateway.	1.1.1.1
Keylife	The Client key life should match the VPN gateway key life.	100
Authentication Key	The Client authentication key should match the VPN gateway authentication key.	ddcHH01887d

Manual key exchange IPSec VPN between two networks

DFL-500 IPSec VPNs can be configured to use Autokey IKE or manual key exchange. In most cases Autokey key exchange is preferred because it is easier to configure and maintain. However, manual key exchange may be necessary in some cases for compatibility with third party VPN products.

Use the following procedures to configure a VPN between two internal networks protected by VPN gateways that use manual key exchange (for an example, see Example VPN between two internal networks). Each internal network can be protected by a DFL-500 VPN gateway or one of the networks can be protected by a third-party VPN gateway.

This section describes:

- Configuring the VPN tunnel
- Adding internal and external addresses
- Adding an IPSec VPN policy

Configuring the VPN tunnel

Complete the following procedure on both VPN gateways.

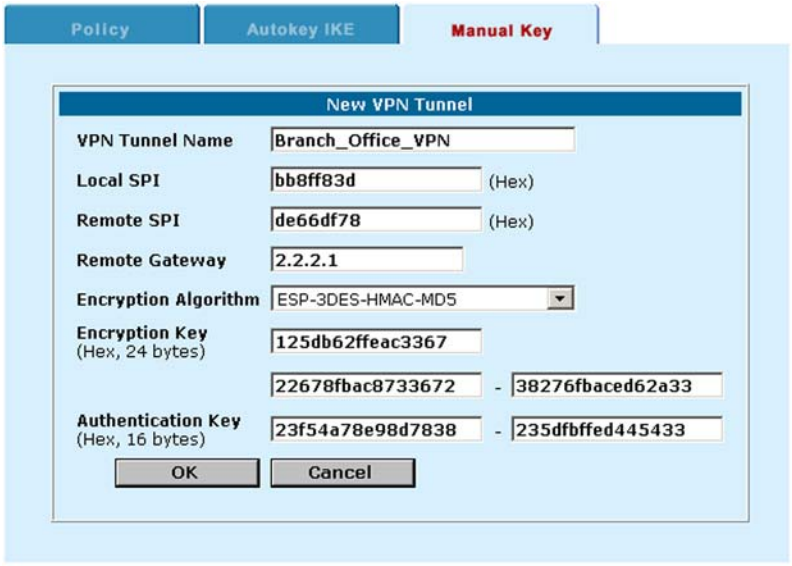
- Go to *VPN* > *IPSEC* > *Manual Key* .
- Click New to add a new manual key VPN tunnel.

- Configure the VPN tunnel.

VPN Tunnel Name	Enter a name for the tunnel. The name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and the @ character are not allowed. If you are configuring a VPN between two DFL-500 gateways, it is recommended that you use the same tunnel name on both sides of the VPN.
Local SPI	(Secure Parameter Index) Enter a hexadecimal number of up to eight digits (digits can be 0 to 9, a to f). This number must be added to the Remote SPI at the opposite end of the tunnel.
Remote SPI	Enter a hexadecimal number of up to eight digits. This number must be added to the Local SPI at the opposite end of the tunnel.
Remote Gateway	Enter the external IP address of the DFL-500 or other IPSec gateway at the opposite end of the tunnel.
Encryption Algorithm	Select an algorithm from the list. Make sure you use the same algorithm at both ends of the tunnel.
Encryption Key	Required for encryption algorithms that include ESP-DES or ESP-3DES. For all DES Encryption algorithms enter one hexadecimal number of up to 16 digits. Use the same encryption key at both ends of the tunnel For all 3DES encryption algorithms enter three hexadecimal numbers of up to 16 digits each. Use the same encryption key at both ends of the tunnel.
Authentication Key	Required for encryption algorithms that include MD5 or SHA1. For MD5 encryption algorithms enter two hexadecimal numbers of 16 digits each. Use the same authentication key at both ends of the tunnel. For SHA1 encryption algorithms, enter two hexadecimal numbers, one of 16 digits and one of 20 digits. Use the same authentication key at both ends of the tunnel.

- Click OK to save the manual key VPN tunnel.

Example manual key exchange VPN tunnel:



Adding internal and external addresses

Use the procedure Adding internal and external addresses to configure the internal and external addresses used by the VPN policy.

Adding an IPSec VPN policy

Use the procedure Adding an IPSec VPN policy to configure the outgoing policy that connects from the local internal network through the VPN tunnel to the remote internal network.

Manual key exchange IPSec VPN for remote clients

Use the following procedures to configure a VPN that allows remote clients to connect to computers on a Main Office internal network (Example VPN between an internal network and remote clients). A remote VPN client can be any computer connected to the Internet and running VPN client software that uses IPSec and manual key exchange. The client must have a static IP address.

Communication between the remote users and the internal network takes place over an encrypted VPN tunnel that connects the remote user to the DFL-500 VPN gateway across the Internet. Once connected to the VPN, the remote user's computer appears as if it is installed on the internal network.

Manual key exchange VPNs do not support VPN clients with dynamic IP addresses.

The VPN client PC must have industry standard VPN client software installed. DFL-500 VPN is based on the industry standard IPSec implementation of VPN making it interoperable with other IPSec VPN products (see Compatibility with third-party VPN products). D-Link recommends SafeNet/Soft-PK from IRE, Inc.

Configuring the VPN tunnel

You can either create multiple VPN tunnels, one for each VPN client, or you can create one VPN tunnel with a remote gateway address set to 0.0.0.0. This VPN tunnel accepts connections from any Internet address.

You must create complementary VPN tunnels on the VPN gateway and the clients. On both, the tunnel must have the same name, keylife, and authentication key.

Complete the following procedure on the DFL-500 VPN gateway.

- Go to *VPN* > *IPSEC* > *Manual Key* .
- Click New to add a new manual key VPN tunnel.
- Configure the VPN tunnel as described in Configuring the VPN tunnel.
- In the Remote Gateway field, enter the external IP address of the VPN client.

  For the example network shown in Example VPN between an internal network and remote clients, you would use 2.2.2.2 as the remote gateway. To accept connections from more than one client, set the Remote Gateway address to 0.0.0.0.
- Click OK to save the manual key VPN tunnel.

Adding internal and external addresses

Use the procedure Adding internal and external addresses to configure the internal and external addresses used by the VPN policy.

Adding an IPSec VPN policy

Use the procedure Adding an IPSec VPN policy to add a VPN policy that associates the source address of the internal network and the destination address of the VPN client with the VPN tunnel created for the VPN client.

Testing a VPN

To confirm that a VPN between two networks has been configured correctly, use the ping command from one internal network to connect to a computer on the other internal network. The IPSec VPN tunnel starts automatically when the first data packet destined for the VPN is intercepted by the DFL-500.

To confirm that a VPN between a network and one or more clients has been configured correctly, start a VPN client and use the ping command to connect to a computer on the internal network. The VPN tunnel initializes automatically when the client makes a connection attempt. You can start the tunnel and test it at the same time by pinging from the client to an address on the internal network.

IPSec VPN pass through

Configure IPSec pass through so that users on your internal network can connect to a VPN on the Internet. VPN pass through allows the VPN connection to pass-through your firewall and connect to the destination VPN. The DFL-500 performs address translation on the connection, so that it seems to the target VPN gateway that the connection to its VPN is originating from the external interface of your DFL-500.

IPSec VPN pass through is only supported in NAT mode.

Use VPN pass through so that:

- A visitor using your internal network can connect through your DFL-500 to their organization's VPN
- A subnet on your Internal network, protected by a VPN gateway, can connect through your DFL-500 to a VPN on the Internet

No special VPN configuration is required for the client or VPN gateway on your internal network. The VPN tunnel configuration of the VPN gateway on the Internet must be changed to accept connections from the IP address of the external interface of the DFL-500.

This section describes how to create two IPSec VPN pass through configurations:

- IPSec client to network VPN pass through
- IPSec network to network VPN pass through

IPSec client to network VPN pass through

Use the following procedure to create the configuration shown in IPSec client connecting to a VPN in the Internet using VPN pass through. In this configuration, the PC on your Internal network runs IPSec VPN client software and connects to a VPN gateway on the Internet.

- Configure the IPSec VPN client to connect to the IPSec VPN gateway as if the client computer is connected directly to the Internet.
- Add the external IP address of the DFL-500 firewall to the destination IPSec VPN gateway. See Adding addresses.
- Configure the destination IPSec VPN Gateway with a VPN tunnel and policy to accept VPN connections from a VPN client with the static IP address of the external interface of the DFL-500 firewall.

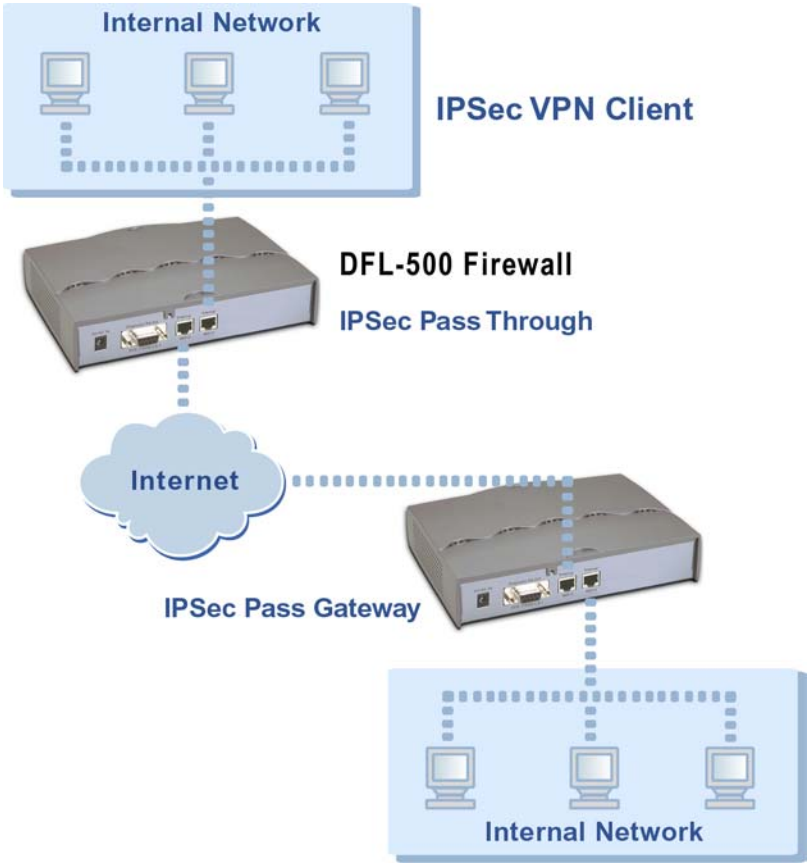
  For more information about configuring the VPN client and IPSec VPN Gateway, see Autokey IPSec VPN for remote clients or Manual key exchange IPSec VPN for remote clients.

- On the DFL-500 firewall, go to ***Firewall > Policy*** .
- Select IPSEC Pass Through and click Apply.

When the IPSec client connects to the IPSec VPN gateway, the DFL-500 firewall accepts IPSec VPN connections from the internal network and performs network address translation on them. The VPN packets

are forwarded to the destination IPSec VPN gateway with a source address of the external interface of the DFL-500 firewall.

IPSec client connecting to a VPN in the Internet using VPN pass through:



IPSec network to network VPN pass through

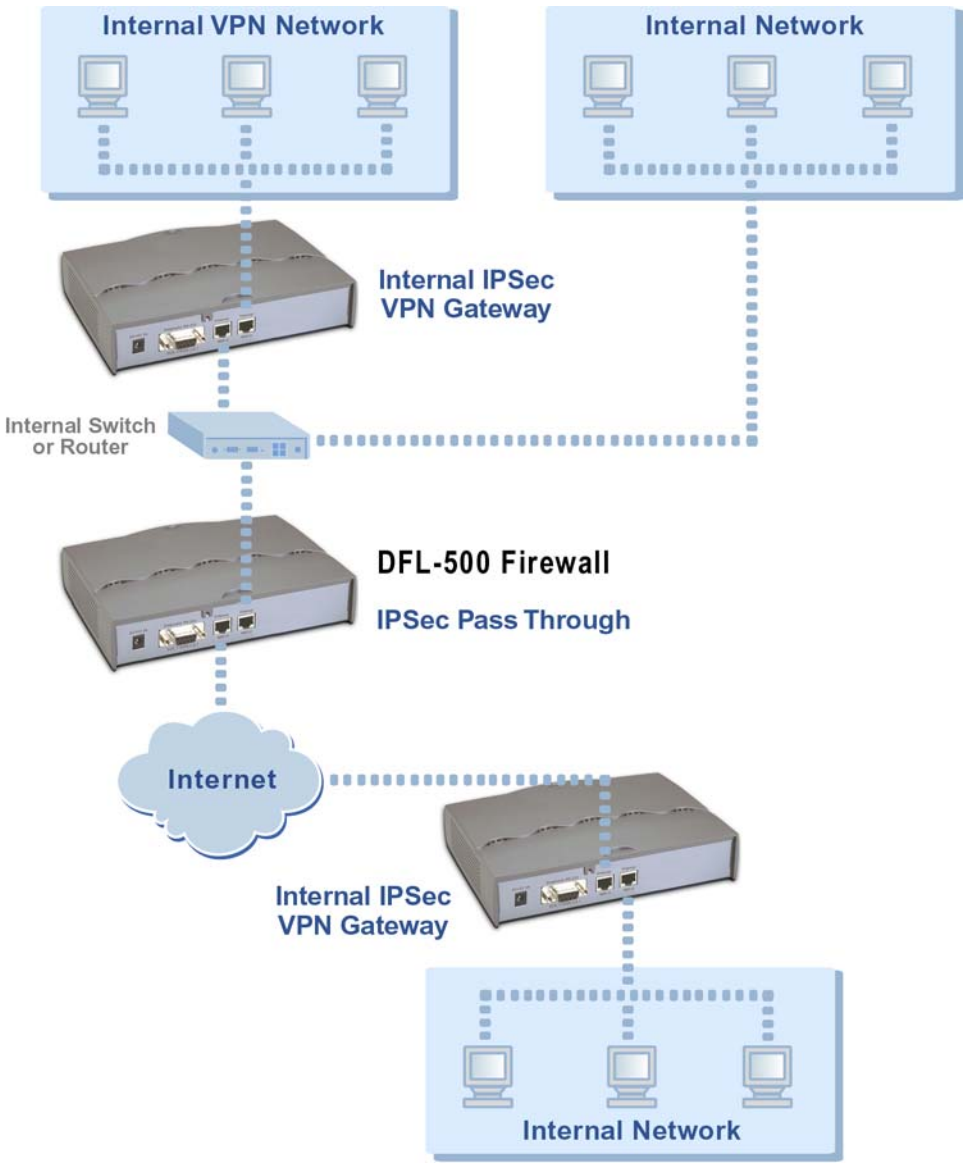
Use the following procedure to create the configuration shown in IPSec network to network VPN pass through. In this configuration, the Internal IPSec VPN gateway connects an Internal network to the destination IPSec VPN gateway on the Internet. The VPN passes through the DFL-500 firewall.

- Configure the Internal IPSec VPN gateway to connect to the destination IPSec VPN gateway as if the Internal IPSec VPN gateway is connected directly to the Internet.
- Add the external IP address of the DFL-500 firewall to the destination IPSec VPN gateway. See Adding addresses.
- Configure the destination IPSec VPN Gateway with a VPN tunnel and policy to accept VPN connections from a VPN gateway with the static IP address of the external interface of the DFL-500 firewall.

For more information about configuring the VPN client and IPSec VPN Gateway, see Autokey IPSec VPN between two networks or Manual key exchange IPSec VPN between two networks.

- On the DFL-500 firewall, go to ***Firewall > Policy*** .
- Select IPSEC Pass Through and click Apply.

IPSec network to network VPN pass through:



When a computer on the internal IPSec VPN network connects to the internal network behind the destination IPSec VPN gateway, the DFL-500 firewall accepts IPSec VPN connections from the internal network and performs network address translation on them. The VPN packets are forwarded to the destination IPSec VPN gateway with a source address of the external interface of the DFL-500 firewall.

PPTP and L2TP VPNs

Using DFL-500 PPTP and L2TP Virtual Private Networking (VPN), you can create a secure connection between a client computer running Windows and an internal network protected by a DFL-500.

PPTP is a Microsoft Windows VPN standard. You can use PPTP to connect computers running Microsoft Windows to a DFL-500-protected private network without using third party VPN client software.

L2TP combines Windows PPTP functionality with IPSec security. L2TP is supported by most recent versions of MS-Windows.

The secure VPN tunnel makes it appear to the user that the client computer is directly connected to the internal network. The VPN protects data passing through the tunnel by encrypting it to guarantee confidentiality. In addition, authentication guarantees that the data originated from the claimed sender and was not damaged or altered in transit.

PPTP and L2TP VPNs are only supported in NAT mode.

This chapter describes:

- PPTP VPN configuration
- PPTP VPN pass through
- L2TP VPN configuration
- RADIUS authentication for PPTP and L2TP VPNs

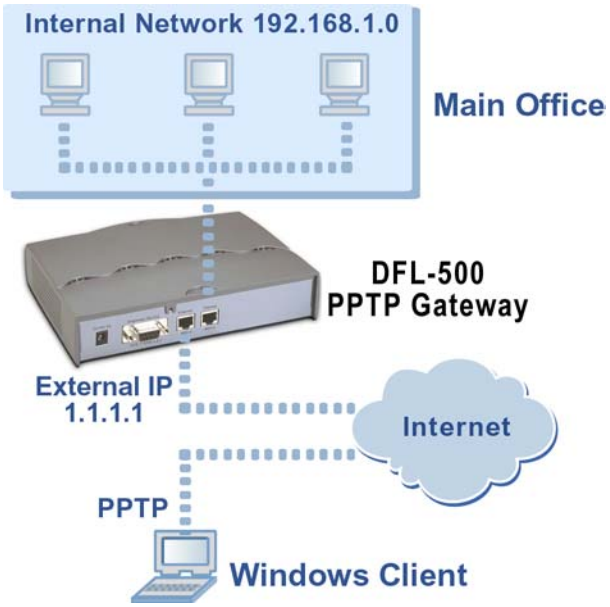
PPTP VPN configuration

This section describes how to configure the DFL-500 as a PPTP VPN server. This section also describes how to configure Windows 98, Windows 2000, and Windows XP clients to connect to the PPTP VPN.

You configure the DFL-500 to support PPTP by adding PPTP users and specifying a PPTP address range. You can also require PPTP VPN users to authenticate to your RADIUS server. Finally, to connect to the PPTP VPN your remote Windows clients must be configured for PPTP.

Make sure that your ISP supports PPTP connections.

PPTP VPN between a Windows client and the DFL-500:



This section describes:

- Configuring the DFL-500 as a PPTP server
- Configuring a Windows 98 client for PPTP
- Configuring a Windows 2000 Client for PPTP
- Configuring a Windows XP Client to connect to a DFL-500 PPTP VPN

Configuring the DFL-500 as a PPTP server

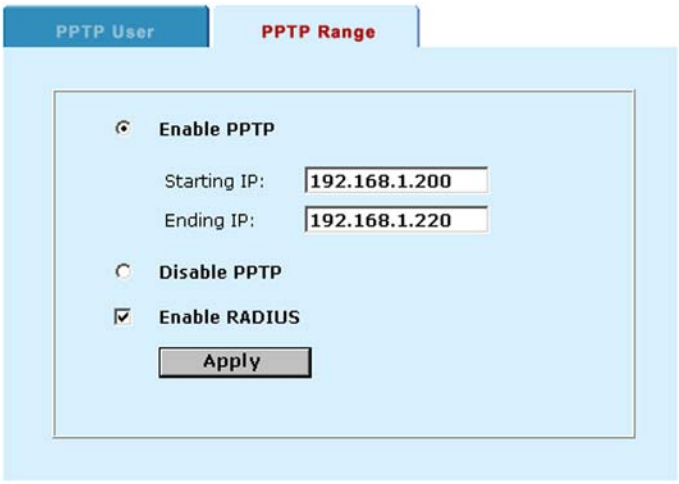
Use the following procedure to configure the DFL-500 to be a PPTP server.

- Go to *VPN* > *PPTP* > *PPTP User* .
- Click New to add a PPTP user name and password.
- Enter a user name and password.
  The user name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and the @ character are not allowed.
  The password must be at least 6 characters long and can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and the @ character are not allowed.
  A client can connect to the PPTP VPN with this user name and password.
- Repeat steps Go to VPN > PPTP > PPTP User. to Enter a user name and password. to add more PPTP user names and passwords as required.
- Go to ***VPN > PPTP > PPTP Range*** .
- Click Enable PPTP.
- Specify the PPTP address range.
  The PPTP address range is the range of addresses on your internal network that must be reserved for remote PPTP clients. When a remote client connects to the internal network using PPTP, the computer is assigned an IP address from this range.
- If you are planning on using RADIUS for authentication, click Enable RADIUS.

To turn on RADIUS support, see RADIUS authentication for PPTP and L2TP VPNs.

- Click Apply to enable PPTP through the DFL-500.

Sample PPTP Range configuration:



Configuring a Windows 98 client for PPTP

Use the following procedure to configure a client machine running Windows 98 so that it can connect to a DFL-500 PPTP VPN. To configure the Windows 98 client, you must install and configure windows dial-up networking and virtual private networking support.

Installing PPTP support

- Go to *Start* > *Settings* > *Control Panel* > *Network* .
- Click Add.
- Choose Adapter.
- Click Add.
- Select Microsoft as the manufacturer.
- Select Microsoft Virtual Private Networking Adapter.
- Click OK twice.
- Insert diskettes or CDs as required.
- Restart the computer.

Configuring a PPTP dial-up connection

- Go to *My Computer* > *Dial Up Networking* .
- Double-click Make New Connection.
- Name the connection and click Next.
- Enter the external IP address or hostname of the DFL-500 to connect to and click Next.
- Click Finish.

  An icon for the new connection appears in the Dial-up networking folder.
- Right click the new icon and select Properties.
- Go to Server Types.
- Uncheck IPX/SPX Compatible.

- Click on TCP/IP Settings.
- Turn off Use IP header compression.
- Turn off Use default gateway on remote network.
- Click OK twice.

Connecting to the PPTP VPN

- Start the dial-up connection that you configured in the previous procedure.
- Enter your PPTP VPN User Name and Password.
- Click Connect.

Configuring a Windows 2000 Client for PPTP

Use the following procedure to configure a client machine running Windows 2000 so that it can connect to a DFL-500 PPTP VPN.

Configuring a PPTP dial-up connection

- Go to *Start* > *Settings* > *Network and Dial-up Connections* .
- Double click Make New Connection to start the Network Connection Wizard. Click Next.
- For Network Connection Type, select Connect to a private network through the Internet and click Next.
- For Destination Address, enter the external address of the DFL-500 to connect to and click Next.
- Set Connection Availability to Only for myself and click Next.
- Click Finish.
- Click Properties in the Connect window.
- Click the Security tab.
- Uncheck Require data encryption.
- Click OK.

Connecting to the PPTP VPN

- Start the dial-up connection that you configured in the previous procedure.
- Enter your PPTP VPN User Name and Password.
- Click Connect.
- In the connect window, enter the User Name and Password you use to connect to your dial-up network connection.

  This user name and password is not the same as your VPN user name and password.

Configuring a Windows XP Client to connect to a DFL-500 PPTP VPN

Use the following procedure to configure a client machine running Windows XP so that it can connect to a DFL-500 PPTP VPN.

Configuring a PPTP dial-up connection

- Go to *Start* > *Control Panel* .
- Click Network and Internet Connections.
- Select Create a Connection to the network of your workplace and click Next.
- Click Virtual Private Network Connection and click Next.

- Name the connection and click Next.
- If the Public Network dialog box appears, choose the appropriate initial connection and click Next.
- In the VPN Server Selection dialog, enter the external IP address or hostname of the DFL-500 to connect to and click Next.
- Click Finish.

Configure the VPN connection

- Right click the icon that you have created.
- Select ***Properties > Security*** .
- Click Typical to configure typical settings.
- Click to select Require data encryption.
- Click Advanced to configure advanced settings.
- Click Settings.
- Click to select Challenge Handshake Authentication Protocol (CHAP).
- Make sure none of the other settings are selected.
- Click the Networking tab.
- Make sure the following are selected:
    - TCP/IP
    - QoS Packet Scheduler
- Make sure the following options are not selected:
    - File and Printer Sharing for Microsoft Networks
    - Client for Microsoft Networks
- Click OK.

Connecting to the PPTP VPN

- Connect to your ISP.
- Start the VPN connection that you configured in the previous procedure.
- Enter your PPTP VPN User Name and Password.
- Click Connect.
- In the connect window enter the User Name and Password you use to connect to your dial-up network connection.

  This user name and password is not the same as your VPN user name and password.

PPTP VPN pass through

Configure PPTP pass through so that users on your internal network can connect to a VPN on the Internet. VPN pass through allows the VPN connection to pass-through your firewall and connect to the destination VPN. The DFL-500 performs address translation on the connection, so that it seems to the target VPN gateway that the connection to its VPN is originating from the external interface of your DFL-500.

PPTP VPN pass through is only supported in NAT mode.

Use PPTP VPN pass through so that:

- A visitor using your internal network can connect through your DFL-500 to their organization's VPN

- A subnet on your Internal network, protected by a VPN gateway, can connect through your DFL-500 to a VPN on the Internet

No special VPN configuration is required for the client or VPN gateway on your internal network. The VPN tunnel configuration of the VPN gateway on the Internet must be changed to accept connections from the IP address of the external interface of the DFL-500.

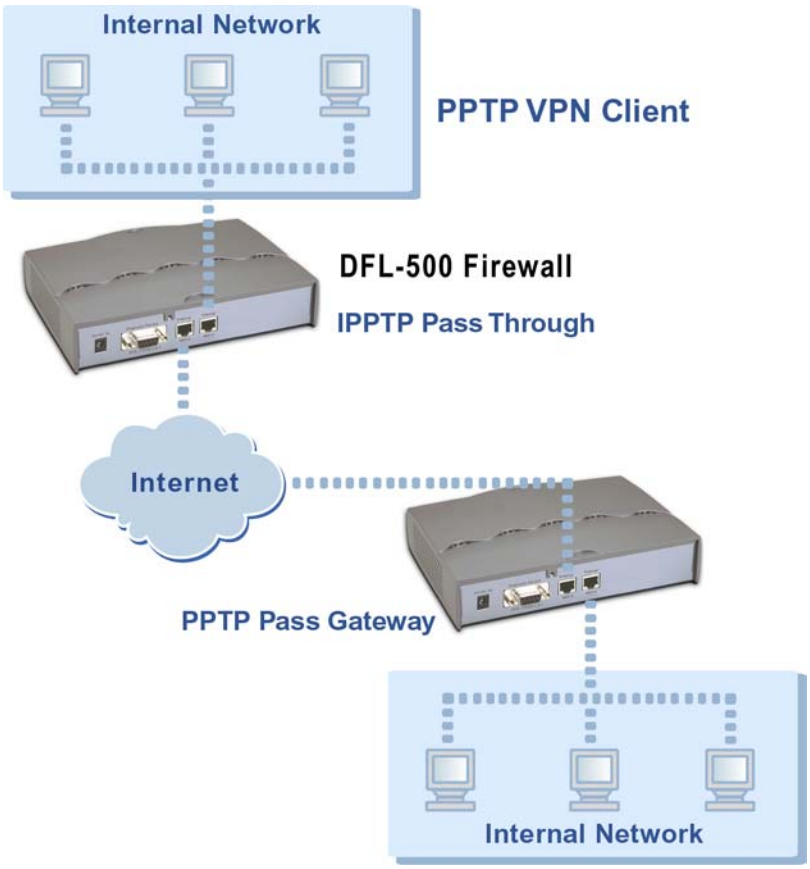
L2TP VPN connections can be made from the internal network to an L2TP VPN gateway on the Internet without modifying the DFL-500 configuration.

This section describes how to create three VPN pass through configurations:

PPTP client to network VPN pass through

Use the following procedure to create the configuration shown in PPTP client connecting to a VPN in the Internet using VPN pass through. In this configuration, the PC on your Internal network runs PPTP VPN client software and connects to the PPTP VPN gateway on the Internet.

PPTP client connecting to a VPN in the Internet using VPN pass through:



- Configure the PPTP VPN client to connect to the destination PPTP VPN gateway as if the client computer is connected directly to the Internet. See PPTP VPN configuration.
- Configure the destination PPTP VPN gateway. See Configuring the DFL-500 as a PPTP server.
- On the DFL-500 firewall, go to ***Firewall > Policy*** .
- Select PPTP Pass Through and click Apply.

When the PPTP VPN client connects to the destination PPTP VPN gateway, the DFL-500 firewall accepts PPTP VPN connections from the internal network and performs network address translation on them. The

VPN packets are forwarded to the PPTP VPN gateway with a source address of the external interface of the DFL-500 firewall.

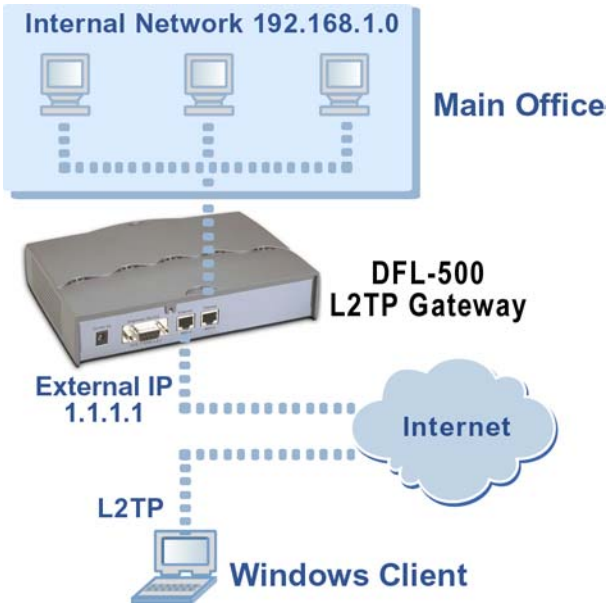
L2TP VPN configuration

This section describes how to configure the DFL-500 as an L2TP VPN server. This section also describes how to configure Windows 2000 and Windows XP clients to connect to the L2TP VPN.

Configuring L2TP is similar to configuring PPTP. You must configure the DFL-500 to support L2TP by adding L2TP users and specifying an L2TP address range. You can also require L2TP VPN users to authenticate to your RADIUS server. Finally, to connect to the L2TP VPN, your remote Windows clients must be configured for L2TP.

Make sure that your ISP supports L2TP connections.

L2TP VPN between a Windows client and the DFL-500:



This section describes:

- Configuring the DFL-500 as an L2TP server
- Configuring a Windows 2000 Client for L2TP
- Configuring a Windows XP Client to connect to a DFL-500 L2TP VPN

Configuring the DFL-500 as an L2TP server

Use the following procedure to configure the DFL-500 to be an L2TP server.

- Go to *VPN* > *L2TP* > *L2TP User* .
- Click New to add an L2TP user name and password.
- Enter a user name and password.

  The user name can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and the @ character are not allowed.

  The password must be at least 6 characters long and can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and the @ character are not allowed.

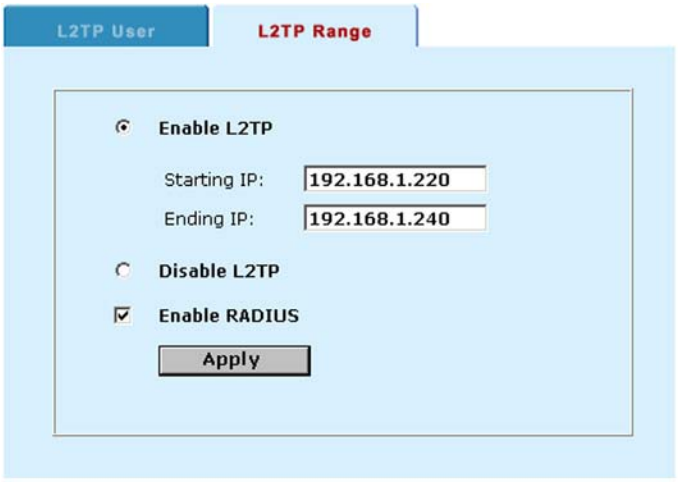
A client can connect to the L2TP VPN with this user name and password.

- Click OK.
- Repeat steps Go to VPN > L2TP > L2TP User. to Click OK. to add more L2TP user names and passwords as required.
- Go to ***VPN > L2TP > L2TP Range*** .
- Click Enable L2TP.
- Specify the L2TP address range.

  The L2TP address range is the range of addresses on your internal network that must be reserved for remote L2TP clients. When a remote client connects to the internal network using L2TP, the computer is assigned an IP address from this range.
- If you are planning on using RADIUS for authentication, click Enable RADIUS.

  To turn on RADIUS support, see RADIUS authentication for PPTP and L2TP VPNs.
- Click Apply to enable L2TP VPNs through the DFL-500.

Sample L2TP Range configuration:



Configuring a Windows 2000 Client for L2TP

Use the following procedure to configure a client machine running Windows 2000 so that it can connect to a DFL-500 L2TP VPN.

Configuring an L2TP dial-up connection

- Go to *Start* > *Settings* > *Network and Dial-up Connections* .
- Double click Make New Connection to start the Network Connection Wizard.
- Click Next.
- For Network Connection Type, select Connect to a private network through the Internet and click Next.
- For Destination Address, enter the external address of the DFL-500 to connect to and click Next.
- Set Connection Availability to Only for myself and click Next.
- Click Finish.
- Click Properties in the Connect window.
- Click the Security tab.
- Make sure Require data encryption is checked.
- Click the Networking tab.

- Set VPN server type to Layer-2 Tunneling Protocol (L2TP).
- Save your changes and continue with the following procedure.

Disabling IPsec

- Click the Networking tab.
- Click Internet Protocol (TCP/IP) properties.
- Double-click the Advanced tab.
- Go to the Options tab and click IP security properties.
- Make sure Do not use IPSEC is checked.
- Click OK and close the connection properties window.

The default Windows 2000 L2TP traffic policy does not allow L2TP traffic without IPSec encryption. You can disable default behavior by editing the Windows 2000 Registry as described in the following steps. Please refer to the Microsoft documentation for editing the Windows Registry.

- Use the registry editor (regedit) to locate the following key in the registry:
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
- Add the following registry value to this key:
  Value Name: ProhibitIpSec
  Data Type: REG_DWORD
  Value: 1
- Save your changes and restart the computer for the changes to take effect.
  You must add the *ProhibitIpSec* registry value to each Windows 2000-based endpoint computer of an L2TP or IPSec connection to prevent the automatic filter for L2TP and IPSec traffic from being created. When the *ProhibitIpSec* registry value is set to 1, your Windows 2000-based computer does not create the automatic filter that uses CA authentication. Instead, it checks for a local or Active Directory IPSec policy.

Connecting to the L2TP VPN

- Start the dial-up connection that you configured in the previous procedure.
- Enter your L2TP VPN User Name and Password.
- Click Connect.
- In the connect window, enter the User Name and Password you use to connect to your dial-up network connection.
  This user name and password is not the same as your VPN user name and password.

Configuring a Windows XP Client to connect to a DFL-500 L2TP VPN

Use the following procedure to configure a client machine running Windows XP so that it can connect to a DFL-500 L2TP VPN.

Configuring an L2TP VPN dial-up connection

- Go to *Start* > *Settings* .
- Click Network and Internet Connections.
- Select Create a connection to the network of your workplace and click Next.
- Click Virtual Private Network Connection and click Next.
- Name the connection and click Next.

- If the Public Network dialog box appears, choose the appropriate initial connection and click Next.
- In the VPN Server Selection dialog, enter the external IP address or hostname of the DFL-500 to connect to and click Next.
- Click Finish.

Configuring the VPN connection

- Right click the icon that you have created.
- Select ***Properties > Security*** .
- Click Typical to configure typical settings.
- Click to select Require data encryption.
- Click Advanced to configure advanced settings.
- Click Settings.
- Click to select Challenge Handshake Authentication Protocol (CHAP).
- Make sure none of the other settings are selected.
- Click the Networking tab.
- Make sure the following are selected:
    - TCP/IP
    - QoS Packet Scheduler
- Make sure the following options are not selected:
    - File and Printer Sharing for Microsoft Networks
    - Client for Microsoft Networks

Disabling IPsec

- Click the Networking tab.
- Click Internet Protocol (TCP/IP) properties.
- Double-click the Advanced tab.
- Go to the Options tab and click IP security properties.
- Make sure Do not use IPSEC is checked.
- Click OK and close the connection properties window.

The default Windows XP L2TP traffic policy does not allow L2TP traffic without IPSec encryption. You can disable default behavior by editing the Windows XP Registry as described in the following steps. Please refer to the Microsoft documentation for editing the Windows Registry.

- Use the registry editor (regedit) to locate the following key in the registry:
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
- Add the following registry value to this key:
  Value Name: ProhibitIpSec
  Data Type: REG_DWORD
  Value: 1
- Save your changes and restart the computer for the changes to take effect.
  You must add the *ProhibitIpSec* registry value to each Windows XP-based endpoint computer of an L2TP or IPSec connection to prevent the automatic filter for L2TP and IPSec traffic from being created. When the *ProhibitIpSec* registry value is set to 1, your Windows XP-based computer does not create the automatic filter that uses CA authentication. Instead, it checks for a local or Active Directory IPSec policy.

Connecting to the L2TP VPN

- Connect to your ISP.
- Start the VPN connection that you configured in the previous procedure.
- Enter your L2TP VPN User Name and Password.
- Click Connect.
- In the connect window, enter the User Name and Password you use to connect to your dial-up network connection.

This user name and password is not the same as your VPN user name and password.

RADIUS authentication for PPTP and L2TP VPNs

If you have RADIUS servers installed, you can configure the DFL-500 to use RADIUS for authenticating PPTP and L2TP users. To configure RADIUS authentication you must add the IP addresses of your RADIUS servers to the DFL-500 VPN configuration and then turn on RADIUS support for PPTP and L2TP.

If you have added PPTP and L2TP user names and passwords and configured RADIUS support, when a PPTP or L2TP user connects to a DFL-500 their user name and password are checked against the DFL-500 PPTP or L2TP user name and password list. If a match is not found locally, the DFL-500 contacts the RADIUS server for authentication.

RADIUS authentication is not supported by Windows 98 clients.

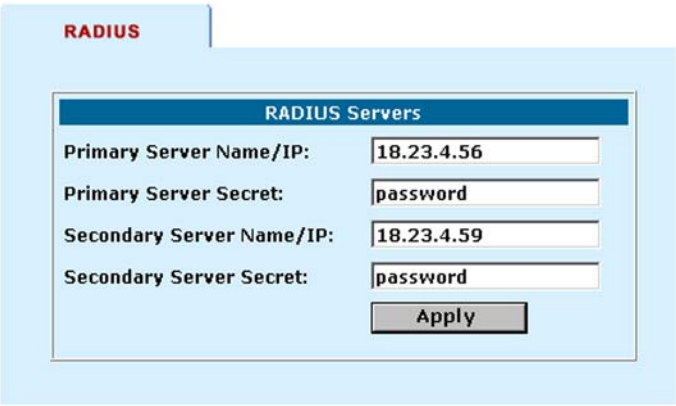
Adding RADIUS server addresses

You can install your RADIUS server on the Internet or on the internal network. No special DFL-500 configuration is required for RADIUS support for PPTP and L2TP other than what is described below. If you want non-VPN users to be able to connect to a RADIUS server installed on your internal network, you must add firewall policies to grant access to the server from the Internet.

To configure the DFL-500 for RADIUS authentication:

- Go to ***VPN > RADIUS*** .
- Enter the server name or IP address of your primary RADIUS server.
- Enter the primary RADIUS server secret.
- Optionally, enter the server name or IP address and secret for your secondary RADIUS server.
- Click Apply.

Example RADIUS configuration:



Turning on RADIUS authentication for PPTP

RADIUS authentication can be turned on separately for PPTP and L2TP. To turn on RADIUS authentication for PPTP users:

- Go to *VPN* > *PPTP* > *PPTP Range* .
- Click to check Enable RADIUS.
- Click Apply.

Turning on RADIUS authentication for L2TP

RADIUS authentication can be turned on separately for PPTP and L2TP. To turn on RADIUS authentication for L2TP users:

- Go to *VPN* > *L2TP* > *L2TP Range* .
- Click to check Enable RADIUS.
- Click Apply.

Intrusion detection system (IDS)

You can configure the IDS to detect and prevent common network attacks and to send an alert email if the IDS detects an attack.

This chapter describes:

- Attack prevention
- Alert email

Attack prevention

With attack prevention configured, the DFL-500 monitors Internet connections for up to 11 common network attacks. If the DFL-500 detects one of these attacks, it takes action to prevent the attack from affecting your Internet connection. All attacks are recorded in the attack log. You can also configure the DFL-500 to send alert emails to system administrators if an attack is detected.

Use the following procedure to configure attack prevention.

- In NAT mode go to *IDS* > *Attack Prevention* .
  In Transparent mode go to ***System > Attack Prevention*** .
- Check the check boxes next to the types of attacks that you want the DFL-500 to detect and prevent.

Attack prevention list:

Alert email

You can configure the DFL-500 to send email alerts to up to three email addresses when the firewall detects an attack from the Internet.

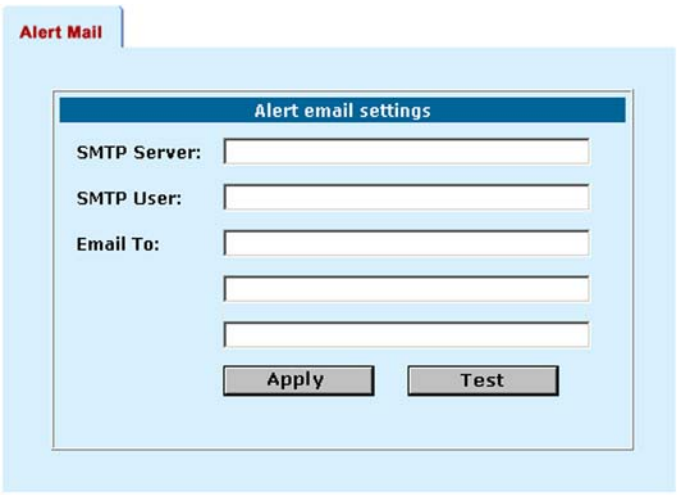
This section describes:

- Configuring alert email
- Testing email alerts

Configuring alert email

- In NAT mode go to *IDS* > *Alert Email* .
  In Transparent mode go to ***System > Config > Alert Mail*** .
- In the SMTP Server field, enter the name of the SMTP server to which the DFL-500 should send email.
  The SMTP server can be located on the internal network or on the Internet.
- In the SMTP User field, enter the email address of a valid user of the SMTP server (for example, user@D-Link.com).
  This is the address that the mail will originate from.
- Enter up to 3 destination email addresses in the Email To fields.
  These are the email addresses that the DFL-500 sends email alerts to.
- Click Apply to save the email alert settings.
- Make sure that the DNS server settings are correct for the DFL-500. See Setting DNS server addresses.
  Because the DFL-500 uses the SMTP server name to connect to the mail server, it must be able to look up this name on your DNS server.

Example alert email settings:



Testing email alerts

You can test your email alert settings by sending a test email.

- Go to *System* > *Config* > *Alert Mail* .
- Click Test to send test email messages from the DFL-500.

Virus protection

D-Link's DFL-500 secure gateway solution adds anti-virus and anti-worm functionality to conventional VPN and firewall technology. Virus and worm protection screens the information found in web traffic (HTTP protocol) and email traffic (SMTP, POP3, and IMAP protocols) for the following types of target files:

- Executable files (exe, bat, and com)
- Visual basic files (vbs)
- Compressed files (zip, gzip, tar, hta, and rar)
- Screen saver files (scr)
- Dynamic link libraries (dll)
- MS Office files

You can configure DFL-500 virus scanning to block target files (high level protection), to scan target files for viruses (medium level protection), or to allow target files through (low level protection).

With high level protection turned on, the DFL-500 identifies and removes all files and attachments from content protocol data streams before they enter your internal network.

With medium level protection turned on, the DFL-500 virus scanning engine scans all target files for viruses. You can configure the virus scanning engine to run a virus signature scan and a macro scan on each target file.

With low level protection turned on, DFL-500 virus protection is temporarily suspended. All target files are forwarded directly to their destinations.

With worm protection turned on, the DFL-500 checks HTTP requests by scanning their originating web page for known worm patterns. To scan email attachments for worms, the DFL-500 looks for filenames known to be used by worms.

If the DFL-500 detects a virus or worm in a file, the file is deleted from the data stream and replaced with an alert message. DFL-500 content virus and worm prevention is transparent to the end user. Client and server programs require no special configuration and D-Link high performance hardware and software ensure there are no noticeable download delays.

This chapter describes:

- Virus protection for your internal network
- Virus protection for incoming connections
- Worm protection
- Updating your antivirus database
- Displaying virus and worm lists

Virus protection is available in NAT mode but not in Transparent mode.

Virus protection for your internal network

You can configure virus protection to screen web traffic (HTTP protocol) and email traffic (SMTP, POP3, and IMAP protocols) for viruses. You can configure high, medium, and low level protection for each of these types of traffic.

Several configuration options are available for each level of virus protection. By changing the protection level and the configuration options for each level, you can quickly and easily react to new virus threats before your network becomes infected.

This section describes:

- High level virus protection for your internal network
- Medium level virus protection for your internal network
- Low level virus protection for your internal network

To protect your internal network from viruses, you must configure ***outgoing*** virus protection. Even though viruses are introduced to your internal network by being downloaded through your firewall, an outgoing connection from your internal network to the web page or email server must first be started. It is this outgoing connection that triggers virus protection.

High level virus protection for your internal network

High level protection removes target files downloaded during web transfers and in email attachments before they enter your private network.

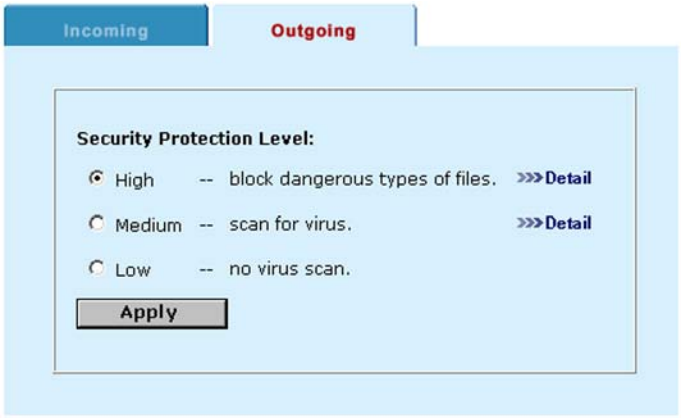
You can switch on high level data protection separately for the HTTP, SMTP, POP3, and IMAP content protocols. For each content type, you can also select target file types to be removed. The virus scanner replaces deleted files with an alert message that is forwarded to the user.

Use High level protection to remove all content that poses a potential threat before it reaches your protected network. This security level provides the best protection from active computer virus attacks. It is also the only protection available from a virus that is so new that no effective virus scanner protects against it. You would not normally run the DFL-500 with high level protection turned on. However, it is available for extremely high risk situations, where there is no other way to prevent viruses from entering your network.

To protect your internal network with high level virus protection:

- Go to *Anti-Virus* > *HTTP* > Outgoing.
- Click High to block files from being downloaded from web pages.

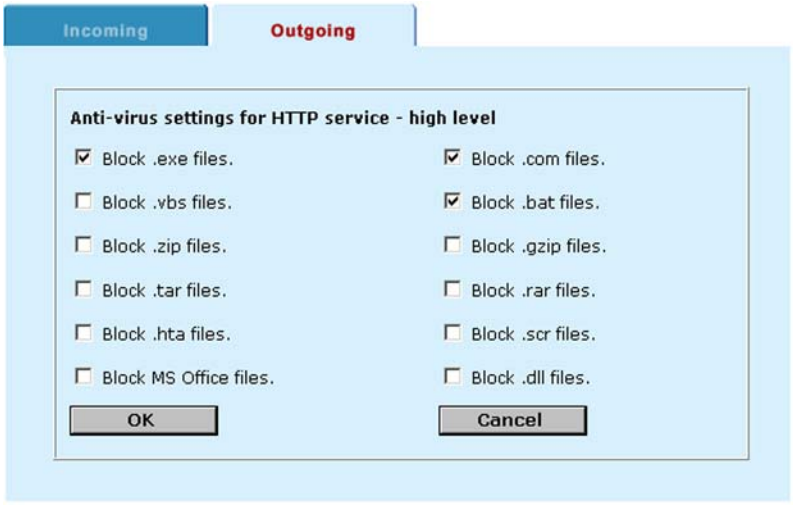
Setting HTTP high level protection



- Click Detail and select the types of files to block.

  By default exe, com, and bat files are blocked. In addition, you can block vbs, zip, tar, hta, gzip, rar, scr, dll, and MS Office files.

Example HTTP high level file blocking configuration



- Click OK and click Apply.
- Go to ***Anti-Virus > SMTP*** > Outgoing and repeat steps Click High to block files from being downloaded from web pages. to Click OK and click Apply. to configure high level virus protection to block the downloading of email attachments in SMTP email traffic.
- Go to ***Anti-Virus > POP3*** > Outgoing and repeat steps Click High to block files from being downloaded from web pages. to Click OK and click Apply. to configure high level virus protection to block the downloading of email attachments in POP3 traffic.
- Go to ***Anti-Virus > IMAP*** > Outgoing and repeat steps Click High to block files from being downloaded from web pages. to Click OK and click Apply. to configure high level virus protection to block the downloading of email attachments in IMAP traffic.

When the DFL-500 blocks a file, the user who requested the file receives the following message:

High Security Alert!!! You are not allowed to download this type of file .

Medium level virus protection for your internal network

Medium level protection scans all target files for viruses. You can configure the DFL-500 to scan target files for virus signatures and macro viruses.

If a virus is found in a file, the virus scanner deletes the file and replaces it with an alert message that is forwarded to the user. If a virus is not found, the file is forwarded unchanged to the user.

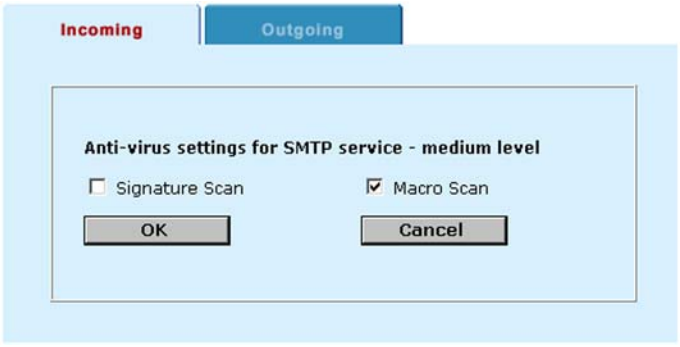
Medium level virus scanning prevents known viruses from entering your internal network while still allowing virus-free HTTP downloads and email attachments to pass through the firewall.

To protect your internal network with medium level virus protection:

- Go to *Anti-Virus* > *SMTP* > Outgoing.
- Click Medium to virus scan target files in email attachments in SMTP traffic.
- Click Detail and select the types of scanning to use:

Signature Scan	Scan the target file for byte-strings that identify known viruses.
Macro Scan	Extract macros from MS Office files and scan them for known macro viruses.

Example SMTP virus protection settings



- Click OK and click Apply.
- Go to ***Anti-Virus > HTTP*** > Outgoing and repeat steps Click Medium to virus scan target files in email attachments in SMTP traffic. to Click OK and click Apply. to configure medium level virus protection to virus scan target files downloaded from Internet web pages.
- Go to ***Anti-Virus > POP3*** > Outgoing and repeat steps Click Medium to virus scan target files in email attachments in SMTP traffic. to Click OK and click Apply. to configure medium level virus protection to virus scan target files in email attachments in POP3 traffic.
- Go to ***Anti-Virus > IMAP*** > Outgoing and repeat steps Click Medium to virus scan target files in email attachments in SMTP traffic. to Click OK and click Apply. to configure medium level virus protection to virus scan target files in email attachments in IMAP traffic.

When the DFL-500 detects a virus and removes the infected file, the user who requested the file receives a message similar to the following:

Sorry, Dangerous Attachment has been removed.
It was infected with the "Generic VBA Virus" virus

Low level virus protection for your internal network

Low level protection suspends virus protection. All target files are forwarded unchanged to their destinations.

To configure low level protection:

- Go to *Anti-Virus* > *HTTP* > Outgoing.
- Click Low to turn off virus scanning for Internet web pages.
- Click Apply.
- Go to ***Anti-Virus > SMTP*** > Outgoing and repeat steps Click Low to turn off virus scanning for Internet web pages. and Click Apply. to turn off virus scanning of SMTP traffic.
- Go to ***Anti-Virus > POP3*** > Outgoing and repeat steps Click Low to turn off virus scanning for Internet web pages. and Click Apply. to turn off virus scanning of POP3 traffic.
- Go to ***Anti-Virus > IMAP*** > Outgoing and repeat steps Click Low to turn off virus scanning for Internet web pages. and Click Apply. to turn off virus scanning of IMAP traffic.

Virus protection for incoming connections

You can prevent the spread of viruses from servers on your internal network by configuring ***incoming*** virus protection. Incoming virus protection can be configured for the following services:

- HTTP, if you have an Internet web server installed on your internal network

- SMTP, to prevent users on your internal network from sending email attachments that contain viruses to addresses on the Internet
- POP3, if you allow users on the Internet to connect to a POP3 server on your internal network
- IMAP, if you allow users on the Internet to connect to an IMAP server on your internal network

Even though viruses are distributed from your internal network by being uploaded through your firewall, an incoming connection to a server on your internal network must first be started. It is this incoming connection that triggers DFL-500 incoming virus protection.

This section describes:

- High level virus protection for incoming connections
- Medium level virus protection for incoming connections
- Low level virus protection for incoming connections

High level virus protection for incoming connections

High level protection removes target files in web transfers and in email attachments before they pass through the firewall.

You can switch on high level data protection separately for the HTTP, SMTP, POP3, and IMAP content protocols. For each content type, you can also select target file types to be removed. The virus scanner replaces deleted files with an alert message that is forwarded to the external user.

To configure high level virus protection to prevent the distribution of viruses from your internal network:

- Go to *Anti-Virus* > *HTTP* > Incoming.
- Click High to block files from being downloaded from your web server to users on the Internet.
- Click Detail and select the types of files to block.

  Configure high level HTTP virus protection if you have an Internet web server on your internal network and you want to prevent users on the Internet from downloading attachments that may contain viruses. By default .exe, .com, and .bat files are blocked. In addition, you can block .vbs, .zip, .tar, .hta, .gzip, .rar, .scr, .dll, and MS Office files.
- Click OK and click Apply.
- Go to ***Anti-Virus > SMTP*** > Incoming and repeat steps Click High to block files from being downloaded from your web server to users on the Internet. to Click OK and click Apply. to configure high level virus protection to block email attachments in SMTP traffic.
- Go to ***Anti-Virus > POP3*** > Incoming and repeat steps Click High to block files from being downloaded from your web server to users on the Internet. to Click OK and click Apply. to configure high level virus protection to block email attachments in POP3 traffic.
- Go to ***Anti-Virus > IMAP*** > Incoming and repeat steps Click High to block files from being downloaded from your web server to users on the Internet. to Click OK and click Apply. to configure high level virus protection to block the downloading of email attachments in IMAP traffic.

When the DFL-500 blocks a file, the user who requested the file receives the following message:

High Security Alert!!! You are not allowed to download this type of file .

Medium level virus protection for incoming connections

Medium level protection scans all target files for viruses. You can configure the DFL-500 to scan target files for virus signatures and macro viruses.

If a virus is found in a file, the virus scanner deletes the file and replaces it with an alert message that is forwarded to the user. If a virus is not found, the file is forwarded unchanged to the user.

Medium level virus scanning prevents known viruses from passing through the firewall from your internal network to the Internet while still allowing virus free HTTP downloads and email attachments to pass through the firewall.

To configure medium level virus protection to prevent the distribution of viruses from your internal network:

- Go to *Anti-Virus* > *HTTP* > Incoming.
- Click Medium to virus scan target files downloaded from your web server to users on the Internet.
- Click Detail and select the types of scanning to use.

Signature Scan	Scan the target file for byte-strings that identify known viruses.
Macro Scan	Extract macros from MS Office files and scan them for known macro viruses.

- Click OK and click Apply.
- Go to ***Anti-Virus > SMTP*** > Incoming and repeat steps See Click Medium to virus scan target files downloaded from your web server to users on the Internet. to See Click OK and click Apply. to configure medium level virus protection to virus scan target files in email attachments in SMTP traffic.
- Go to ***Anti-Virus > POP3*** > Incoming and repeat steps See Click Medium to virus scan target files downloaded from your web server to users on the Internet. to See Click OK and click Apply. to configure medium level virus protection to virus scan target files in email attachments in POP3 traffic.
- Go to ***Anti-Virus > IMAP*** > Incoming and repeat steps See Click Medium to virus scan target files downloaded from your web server to users on the Internet. to See Click OK and click Apply. to configure medium level virus protection to virus scan target files in email attachments in IMAP traffic.

When the DFL-500 detects a virus and removes the infected file, the user who requested the file receives a message similar to the following:

Sorry, Dangerous Attachment has been removed.
It was infected with the "Generic VBA Virus" virus

Low level virus protection for incoming connections

Incoming low level protection suspends virus protection. All target files are forwarded unchanged to their destinations.

To configure incoming low level protection:

- Go to *Anti-Virus* > *HTTP* > Incoming.
- Click Low to turn off virus scanning for Internet web pages.
- Click Apply.
- Go to ***Anti-Virus > SMTP*** > Incoming and repeat steps See Click Low to turn off virus scanning for Internet web pages. and See Click Apply. to turn off virus scanning for email attachments in SMTP traffic.
- Go to ***Anti-Virus > POP3*** > Incoming and repeat steps See Click Low to turn off virus scanning for Internet web pages. and See Click Apply. to turn off virus scanning for email attachments in POP3 traffic.
- Go to ***Anti-Virus > IMAP*** > Incoming and repeat steps See Click Low to turn off virus scanning for Internet web pages. and See Click Apply. to turn off virus scanning for email attachments in IMAP traffic.

Worm protection

You can configure worm protection to screen web and email traffic to prevent worms from infecting your internal network.

This section describes:

- Worm protection for your internal network
- Worm protection for incoming connections

Worm protection for your internal network

When configured for worm protection, the virus scanning engine checks HTTP requests by scanning their originating web page for known worm patterns. For example, Code Red attempts to gain entry to MS IIS servers by trying to exploit a known buffer overflow bug in these servers.

To scan SMTP, POP3, and IMAP email attachments for worms, the virus scanning engine looks for filenames known to be used by worms. For example, the Nimda worm uses files named readme.exe and sample.exe.

If the virus scanning engine detects a worm, the file is deleted and replaced with an alert message.

To protect your internal network from worms, you must configure ***outgoing*** worm protection. Even though worms are introduced to your internal network by being downloaded through your firewall, an outgoing connection from your internal network to the web page or email server must first be started. It is this outgoing connection that triggers worm protection.

To protect your internal network from worms:

- Go to *Anti-Virus* > *Config* > Worm Protection.
- Click Enable Worm Protection for Incoming Traffic to protect your internal network from worms.
- Click Apply.

Worm protection for incoming connections

When configured for worm scanning, the virus scanning engine checks HTTP requests for worms by scanning their originating web page for known worm patterns. For example, Code Red attempts to gain entry to MS IIS servers by trying to exploit a known buffer overflow bug in these servers.

To scan SMTP, POP3, and IMAP email attachments for worms, the virus scanning engine looks for filenames known to be used by worms. For example, the Nimda worm uses files named readme.exe and sample.exe.

If the virus scanning engine detects a worm, the file is deleted and replaced with an alert message.

Even though worms are distributed from your internal network by being uploaded through your firewall, an incoming connection to a server on your internal network must first be started. It is this incoming connection that triggers DFL-500 incoming virus protection.

To prevent the distribution of worms from servers on your internal network to the Internet:

- Go to *Anti-Virus* > *Config* > Worm Protection.
- Click Enable Worm Protection for Outgoing Traffic to scan content from web servers on your internal network for worms before that content passes through the firewall.
- Click Apply.

Updating your antivirus database

The antivirus database contains the information the virus scanning engine uses to scan files for viruses and worms. This database is continuously updated by D-Link as new viruses and worms are encountered and defined.

You should keep your antivirus database up to date so that the DFL-500 can protect your network from new viruses. You can update your antivirus database manually, or you can configure the DFL-500 to update the antivirus database automatically.

This section describes:

- Manual antivirus database updates
- Automatic antivirus database updates

Manual antivirus database updates

Use the following procedure to update your antivirus database manually. This procedure restarts the DFL-500.

If you have configured automatic virus database updates, you can also manually update your antivirus database by going to ***Anti-Virus > Config > Update*** and clicking Update Now.

- Download the latest antivirus database from the D-Link support website at http://tsd.dlink.com.tw and copy it to the computer that you use to connect to the DFL-500 web-based manager.
- Start the DFL-500 web-based manager and go to ***System > Status*** .
- To the right of the Antivirus Database Version click Antivirus Database Update .
- Enter the path and filename for the antivirus database file, or click Browse and locate the file.
- Click OK to upload the antivirus database to the DFL-500.

  The DFL-500 uploads the antivirus database and restarts. This takes about 1 minute.
- Go to ***System > Status*** to confirm that the Antivirus Database Version information has been updated.

When a new virus protection database is made available by D-Link, you should upgrade your DFL-500 as soon as possible. If a new virus is reported and you are not able to upgrade the anti-virus database immediately, you can use the procedure See High level virus protection for your internal network to provide temporary added protection. Because this procedure results in the blocking of all files that might be dangerous, whether they are infected or not, there may be some inconvenience to users.

Automatic antivirus database updates

You can configure the DFL-500 to automatically check an update center to see if a new version of the antivirus database is available. If it finds a new version the DFL-500 automatically downloads and installs the updated database.

You can specify the IP addresses of two update centers and configure the DFL-500 to check and download updated databases once a day, once a week, or once a month.

The DFL-500 writes a message to the event log when it checks for antivirus updates. When The DFL-500 downloads a new version of the antivirus database it also records an event log message and sends an Alert email.

To configure antivirus updates:

- Go to *Anti-Virus* > *Config* > *Update* .
- Enter the IP address or domain name of one or two antivirus database update centers.
- Click to select Periodic Update to turn on the automatic antivirus database updates.
- Specify whether to check for and download updates:

  Daily Once a day.

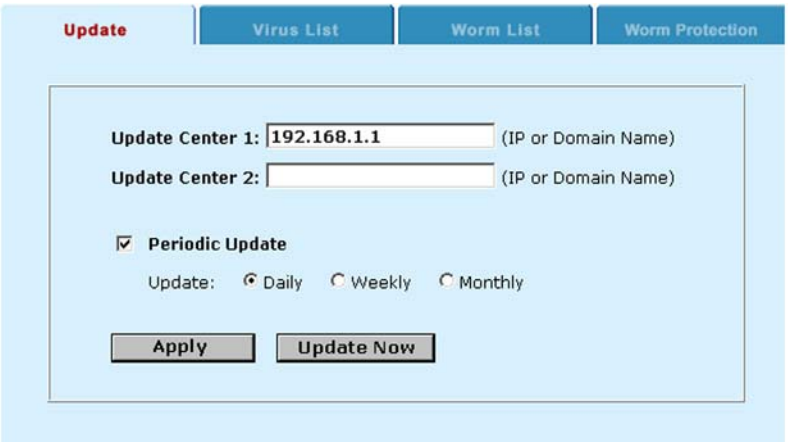
  Weekly Once a week.

  Monthly Once a month.
- Click Apply to save your changes.

  The next antivirus database update takes place in one day, week, or month from the time at which you saved your changes.

At any time, you can click Update Now to update your anti-virus database immediately by downloading the latest database from one of the configured update centres.

Configuring automatic antivirus database updates



Displaying virus and worm lists

Use the following procedure to display the lists of viruses and worms in the antivirus database:

- To display the virus list, go to *Anti-Virus* > *Config* > *Virus List* .
- Scroll through the virus list to view the names of all of the viruses in the list.
- To display the worm list, go to *Anti-Virus* > *Config* > *Worm List* .
- Scroll through the worm list to view the names of all of the worms in the lists.

Web content filtering

Use DFL-500 Web content filtering to block Web sites containing unwanted content. You can configure the DFL-500 to:

- Block web pages that contain unwanted content
- Block access to Internet sites
- Remove scripts from web pages

Web content filtering is only supported in NAT mode.

Block web pages that contain unwanted content

Block web pages that contain content that you want to keep out of your internal network by enabling content blocking and then creating a list of banned words. With content blocking enabled and a list of banned words in place, the DFL-500 blocks access to all web content that contains any of the banned words.

This section describes:

- Enabling the banned word list
- Adding words to the banned word list
- Temporarily disabling the banned word list
- Temporarily disabling individual words in the banned word list
- Clearing the banned word list
- Creating the banned word list using a text editor

Enabling the banned word list

Use the following procedure to turn on content blocking by enabling the banned word list.

From the web-based manager:

- Go to *Web Filter* > *Content Block* .
- Click Enable Banned Word to enable content blocking.

The DFL-500 is now configured to block web pages containing words added to the banned word list.

Adding words to the banned word list

Use the following procedure to add words to the banned word list after content blocking has been enabled.

From the web-based manager:

- Go to *Web Filter* > *Content Block* .
- Click New to add a word to the banned word list.
- Choose a character set for the banned word.

  You can choose Western, Simplified Chinese, Traditional Chinese, Japanese, or Korean.
- Type the banned word.

  Your computer and web browser must be configured to enter characters in the character set that you have chosen.
- Click OK.
- Click the check box beside the word so that DFL-500 blocks web pages containing this word.

- Repeat these steps to add all of the required banned words.

You can also add words to the banned word list by entering them into a text file and then uploading the text file to the DFL-500. See Creating the banned word list using a text editor.

Temporarily disabling the banned word list

- Go to *Web Filter* > *Content Block* .
- Uncheck Enable Banned Word to disable content blocking.

Temporarily disabling individual words in the banned word list

- Go to *Web Filter* > *Content Block* .
- Uncheck the check box by individual words in the list so that web pages containing these words are not blocked by the DFL-500.

Clearing the banned word list

Use the following procedure to remove all of the words from the banned words list.

- Go to *Web Filter* > *Content Block* .
- Click Delete to remove all of the words in the banned word list.

Creating the banned word list using a text editor

You can create a list of banned words in a text editor and then upload this text file to the DFL-500.

- In a text editor, create the list of banned words.
  Type one word on each line in the text file. Follow the word with a space and a 1 to enable or a zero (0) to disable the banned word.
  You can enter Western, Simplified Chinese, Traditional Chinese, Japanese, or Korean text.
- Go to ***Web Filter > Content Block*** .
- Click Upload Banned Word list to upload your banned word list.
- Enter the path and filename of your banned word list text file, or click Browse and locate the file.
- Click OK to upload your banned word list text file to the DFL-500.
  The DFL-500 uploads the file.
- Click Return to display the updated list of banned words.
- You can continue to maintain the banned word list by making changes to the text file and uploading it again.

All changes made to the banned word list from the web-based manager are lost when you upload a new banned word list.

Downloading the banned word list

If you make changes to the banned word list using the web-based manager, you can download the banned word list to a text file:

- Go to *Web Filter* > *Content Block* .

- Click Download Banned Word list to download the banned word list to your management computer.

The DFL-500 downloads the banned word list to a text file on the management computer.

Block access to Internet sites

To block access to internet sites, enable URL blocking and then create a list of URLs and URL patterns to be blocked. With URL blocking enabled and a list of URLs to be blocked, the DFL-500 blocks access to all web pages with the specified URLs or URL patterns.

This section describes:

- Enabling the URL block list
- Adding URLs to the URL block list
- Temporarily disabling the URL block list
- Temporarily disabling blocking individual URLs
- Clearing the URL block list
- Creating the URL block list using a text editor

Enabling the URL block list

Use the following procedure to turn on URL blocking by enabling the URL block list.

From the web-based manager:

- Go to *Web Filter* > *URL Block* .
- Click Enable URL Block to enable content blocking.

The DFL-500 now blocks web pages with URLs or patterns in the URL block list.

Adding URLs to the URL block list

Use the following procedure to add URLs and URL patterns to the URL block list.

- Go to *Web Filter* > *URL Block* .
- Click New to add a URL or URL pattern to the URL block list.
- Type the URL or URL pattern to block.

  Enter a complete URL to block access to a single Internet site only. For example, www.badsite.com blocks access to all of the pages on the badsite web site.

  Enter a pattern to block access to all web sites with that pattern in their URL. For example, "bad" blocks access to any web site with "bad" in it's URL. This would include: www.bad.com, www.bad.org, and sites with names like www.badstuff.com.

  Choose the patterns that you add to this list with care. Adding a word like bad would also block the Carlesbad caves web site.

  You can use regular expressions for more complex pattern matching.
- Click the check box beside the URL or pattern so that the DFL-500 blocks web pages with this URL or pattern.
- Repeat these steps to add all of the required URLs and patterns.

You can also add URLs to the URL block list by entering them into a text file and then uploading the text file to the DFL-500. See Creating the URL block list using a text editor.

Temporarily disabling the URL block list

- Go to *Web Filter* > *URL Block* .
- Uncheck Enable URL Block to disable the URL blocking.

Temporarily disabling blocking individual URLs

- Go to *Web Filter* > *URL Block* .
- Uncheck the check box by individual URLs in the list so that web pages from these URLs are not blocked by the DFL-500.

Clearing the URL block list

Use the following procedure to remove all of the URLs and patterns from the URL block list.

- Go to *Web Filter* > *URL Block* .
- Click Delete to remove all of the URLs from the URL block list.

Creating the URL block list using a text editor

You can create a URL block list in a text editor and then upload this text file to the DFL-500.

- In a text editor, create the list of URLs and patterns to block.

  Type one URL or pattern on each line in the text file. Follow the entry with a space and a 1 to enable or a zero (0) to disable the blocked URL.
- Using the web-based manager, go to ***Web Filter > URL Block*** .
- Click Upload URL Block list to upload your list.
- Enter the path and filename of your URL block list text file, or click Browse and locate the file.
- Click OK to upload the file to the DFL-500.

  The DFL-500 uploads the file.
- Click Return to display the updated URL block list.
- You can continue to maintain the URL block list by making changes to the text file and uploading it again.

All changes made to the URL block list from the web-based manager are lost when you upload a new list.

Downloading the URL block list

If you make changes to the URL block list using the web-based manager, you can download the list to a text file using the following procedure:

- From the web-based manager, go to *Web Filter* > *URL Block* .
- Click Download URL Block list to download the list to your management computer.

The DFL-500 downloads the list to a text file on the management computer.

Remove scripts from web pages

Use the following procedure to configure the DFL-500 to remove scripts from web pages. You can configure the DFL-500 to block Java Applets, Cookies, Malicious Scripts and ActiveX.

Blocking of any of these items may prevent some web pages from working properly.

- Go to *Web Filter* > *Script Filter* .
- Click the filtering options that you want to enable.
- Click Apply to enable script filtering.

Example Script Filter settings to block Java Applets and ActiveX

Logging and reporting

You can configure the DFL-500 to record 3 types of logs:

- Traffic logs record all traffic that attempts to connect through the DFL-500
- Event logs record changes to the system configuration
- Attack logs record network events that appear to be attacks on the DFL-500

This chapter describes:

- Configuring logging
- Log message formats

Configuring logging

You can configure logging to record logs on a remote computer. You can also configure the kind of information that is logged.

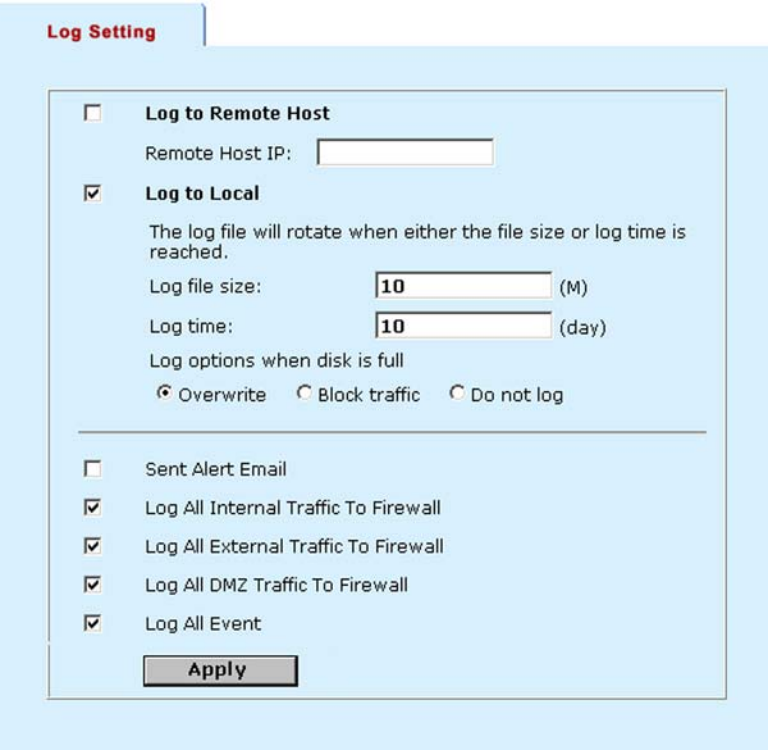
- Recording logs on a remote computer
- Selecting what to log

Recording logs on a remote computer

Use the following procedure to configure the DFL-500 to record logs onto a remote computer. To save log messages to this remote computer it must be configured with a syslog server.

- Go to *Log&Report* > *Log setting* .
- Click Log to Remote Host to send the logs to a remote syslog server.
- Add the IP address of the remote computer to use as a syslog server.
- Click Apply to save your logging settings.

Example log settings



Selecting what to log

Use the following procedure to configure the type of information recorded in DFL-500 logs.

When running in Transparent mode, the DFL-500 only supports Log All Internal Traffic to Firewall, Log All External Traffic to Firewall, and Log All Events.

- Go to *Log&Report > Log setting* .
- Click Sent Alert Email to add an entry to the event log whenever the DFL-500 sends an alert email.
- Click Log All Internal Traffic To Firewall to record all connections to the internal interface. This includes all connections for management.
- Click Log All External Traffic To Firewall to record all connections to the external interface.
- Click Log All Events to record all the changes made to the DFL-500 configuration.
- Click Apply to save your logging settings.

Log message formats

The DFL-500 records three types of logs. Each log type has its own message format. The three formats are:

- Traffic log message format
- Event log message format
- Attack log message format

Traffic log message format

Traffic logs record each connection made to a DFL-500 interface. Each traffic log message records the date and time at which the connection was made, the source and destination address of the connection, and whether the connection was accepted or denied by the firewall.

Traffic log messages are created if you select one or more of the following log settings:

- Log All Internal Traffic to Firewall
- Log All External Traffic to Firewall

Traffic log messages are also created when a policy that is set to log traffic processes a connection.

A sample traffic log message contains the following information:

2002 Mar 25 09:50:47 TCP 192.168.1.23:60932=>192.168.1.99:47873 ACCEPT

Traffic log message format describes the traffic log message format.

Traffic log message format

Description	Format	Example	Maximum Length
Date and time the log message was recorded	*YYYY MMM DD hh:mm:ss*	*2002 Mar 25 09:50:47*	21 bytes
Protocol	*TCP*, *UDP*, or *ICMP*	*TCP*	5 bytes
Source IP address and port number	*ipaddress:port*	*192.168.1.23:60932*	21 bytes
Destination IP and port	*ipaddress:port*	*192.168.1.99:47873*	21 bytes
TCP flag (optional)	*FIN* or *SYN*		3 bytes
Action	*ACCEPT* or *DENY*	*ACCEPT*	6 bytes

Event log message format

Event logs record changes made to the DFL-500 configuration using the web-based manager. Each event log message records the date and time at which the change was made, a description of the change, and the IP address of the management computer from which the change was made.

Event log messages are created if you select the Log All Event setting.

A sample Event log message contains the following information:

2002 Mar 25 09:50:56 Log-Event elong delete successful at 192.168.1.23 by admin

Event log message format describes the event log message format.

Event log message format

Description	Format	Example	Maximum Length
Date and time the log message was recorded	*YYYY MMM DD hh:mm:ss*	*2002 Mar 25 09:50:56*	21 bytes
Event description	*description*	*Log-Event elog delete*	21 bytes
Result	*successful* or *failed*	*successful*	10 bytes
IP address from which the event was received	*at ipaddress*	*at 192.168.1.23*	20 bytes
Administrative user that caused the event	by adminuser	by admin	20 bytes

Attack log message format

Attack logs record attacks made on the DFL-500. Each attack log message records the date and time at which the attack was made, a description of the attack, and the IP address of the computer from which the attack originated.

When running in Transparent mode, the DFL-500 does not create an Attack log.

Attack log messages are created when the DFL-500 detects one of the attacks listed on the ***IDS > Attack Prevention*** page.

A sample attack log message contains the following information:

Jan 23 11:11:28 2002 Attack port scan between Wed Jan 23 11:06:55 2002 and Wed Jan 23 11:06:28 2002 from 23.24.26.78 to 216.21.152.65 tcp port 2765 to 27702

Attack log message format describes the attack log message format.

Attack log message format

Description	Format	Example	Maximum Length
Date and time the log message was recorded	*MMM DD hh:mm:ss*	*Jan 23 11:11:28*	15 bytes
Message describing type of attack	*message*	*Attack port scan*	
Start and end times of attack	*between DDD MMM DD hh:mm:ss YYYY and DDD MMM DD hh:mm:ss YYYY*	*between Wed Jan 23 11:06:55 2002 and Wed Jan 23 11:06:28 2002*	
Source address of the attack.	*from ipaddress*	*from 23.24.26.78*	
Destination address of the attack	*to ipaddress*	*to 216.21.152.65*	
Protocol used for the attack.	*tcp* , *udp* , or *icmp*	*tcp*	5 bytes
Port range of the attack	*port to port*	*2765 to 27702*	

Administering the DFL-500

This chapter describes how to use the DFL-500 web-based manager to administer and maintain the DFL-500. It contains the following sections:

- Logging into the web-based manager
- System status
- Network configuration
- System configuration

Logging into the web-based manager

To connect to the DFL-500 using the web-based manager you require:

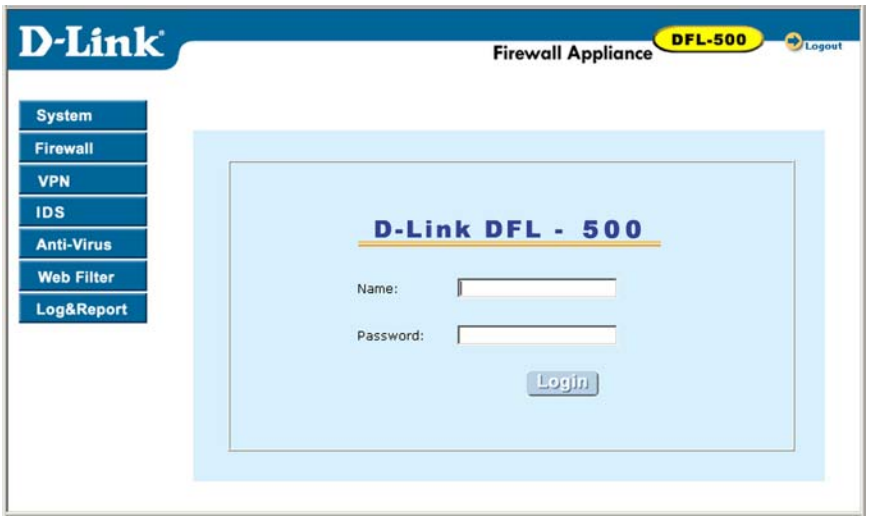
- A computer with an ethernet connection
- Internet Explorer version 4.0 or higher
- A crossover cable or an ethernet hub and two ethernet cables

To connect to the web-based manager:

- Make sure the computer from which you are going to connect to the web-based manager is correctly configured on the same network as the DFL-500 interface to which you are going to connect.
    - If the DFL-500 is running in NAT mode, connect to the internal interface
    - If the DFL-500 is running in Transparent Mode, connect to the management interface
- Start Internet Explorer and browse to the address ***https://address*** . Where ***address*** is the IP address of the internal or management interface to which you are connecting.

The DFL-500 login page appears.

DFL-500 login page



- Type an administrator name and password and click Login.

System status

Go to ***System > Status*** to make any of the following changes to the DFL-500 system status:

- Changing the operating mode
- Upgrading the DFL-500 firmware
- Updating your antivirus database
- Displaying the DFL-500 serial number
- Backing-up system settings
- Restoring system settings
- Restoring system settings to factory defaults
- Restarting the DFL-500
- Shutting down the DFL-500
- System status monitor

Changing the operating mode

Use the following procedure to switch the operating mode of the DFL-500 between NAT mode and Transparent mode.

- Go to *System* > *Status* .
- Click Change Operation Mode .
- Choose an operation mode and click OK.
  The DFL-500 changes operation mode.
- Change your connection to the DFL-500 to be able to reconnect to the web-based manager.
  - In NAT mode connect to the Internal interface
  - In Transparent mode connect to the management interface

Upgrading the DFL-500 firmware

D-Link releases new versions of the DFL-500 firmware periodically. When D-Link releases new firmware, you can download the upgrade from our Web site (http://www.DLink.com). You can save this file on your management computer and then use the following procedure to upgrade the firmware on your DFL-500.

- Go to *System* > *Status* .
- Click Firmware Upgrade .
- Enter the path and filename of the firmware update file, or click Browse and locate the file.
- Click OK to upload the firmware update file to the DFL-500.
  The DFL-500 uploads the file and restarts the DFL-500 running the new version of the firmware.
- Reconnect to the web-based manager.
- Go to ***System > Status*** and check the Firmware Version to confirm that the updated firmware has been installed successfully.

Updating your antivirus database

This procedure is described in Updating your antivirus database.

Displaying the DFL-500 serial number

- Go to *System* > *Status* .

The serial number does not change with firmware upgrades.

Backing-up system settings

This procedure does not back-up the Web content filtering lists. To back-up these lists see Downloading the banned word list and Downloading the URL block list.

You can back-up system settings by downloading them to a text file on the management computer.

- Go to *System* > *Status* .
- Click System Settings Download.
- Click Download System Settings.
- Specify a name and location for the file.
  The system settings file is downloaded to the management computer.
- Click Return to go back to the Status tab.

Restoring system settings

This procedure does not restore the Web content filtering lists. To restore these lists see Creating the URL block list using a text editor and Creating the banned word list using a text editor.

You can restore system settings by uploading to the DFL-500 a previously downloaded system settings text file.

- Go to *System* > *Status* .
- Click System Settings Upload.
- Enter the path and filename of the system settings file, or click Browse and locate the file.
- Click OK to upload the system settings file to the DFL-500.
  The DFL-500 uploads the file and restarts, loading the new system settings.
- Reconnect to the web-based manager and review your configuration to confirm that the uploaded system settings have taken effect.

Restoring system settings to factory defaults

Use the following procedure to restore system settings to the values set at the factory. This procedure does not change the version of the Firmware or the Antivirus database.

This procedure deletes all of the changes that you have made to the DFL-500 configuration and reverts the system to its original configuration including resetting interface addresses.

- Go to *System* > *Status* .
- Click System Settings Reset to Default.
- Click OK to confirm.
  The DFL-500 reverts to the factory configuration file and restarts.
- Reconnect to the web-based manager and review the system configuration to confirm that it has been reset to the default settings.

You can restore your system settings by uploading a previously downloaded system settings text file to the DFL-500.

Default NAT mode system configuration

When the DFL-500 is first powered up or when it is reset to default, the system has the following standard configuration:

- Operation Mode: Network Address Translation
- Internal Address: 192.168.1.99, mask 255.255.255.0
- External Address: 192.168.100.99, mask 255.255.255.0
- Management Address: 10.10.10.1, mask 255.255.255.0
- Administrator Name: admin, Password: blank
- Idle time out: 5 minutes
- Auth time out: 15 minutes
- Internal administration: HTTPS enabled, PING enabled, SSH disabled
- External administration: HTTPS disabled, PING enabled, SSH disabled
- DHCP server: disabled
- SNMP: disabled
- All outgoing traffic: allowed
- All incoming traffic: blocked
- Internal Address: Internal_All
- External Address: External_All
- One-time schedule: none
- Recurring schedule: Always
- Anti-virus for HTTP: Low
- Anti-virus for POP3, SMTP, and IMAP: Low
- Worm protection: Disabled

Default Transparent mode system configuration

When the DFL-500 is first switched to transparent mode or when it is reset to default and run in Transparent mode, the system has the following standard configuration:

- Administrator Name: admin, Password: blank
- Idle Time-out: 5 minutes
- Management Address: 192.168.1.99, mask 255.255.255.0
- Management administration: HTTPS enabled, PING enabled, SSH enabled
- SNMP: disabled
- All outgoing traffic: allowed
- All incoming traffic: blocked
- Internal Address: Internal_All
- External Address: External_All
- One-time schedule: none
- Recurring schedule: Always

Restarting the DFL-500

Use the following procedure to restart the DFL-500 from the web-based manager.

- Go to *System* > *Status* .
- Click Restart.

The DFL-500 restarts.

Shutting down the DFL-500

Use the following procedure to shutdown the DFL-500 from the web-based manager.

- Go to *System* > *Status* .
- Click Shutdown.

The DFL-500 shuts down and all traffic flow through the firewall stops.

The DFL-500 can only be restarted after shutdown by turning the power off and on.

System status monitor

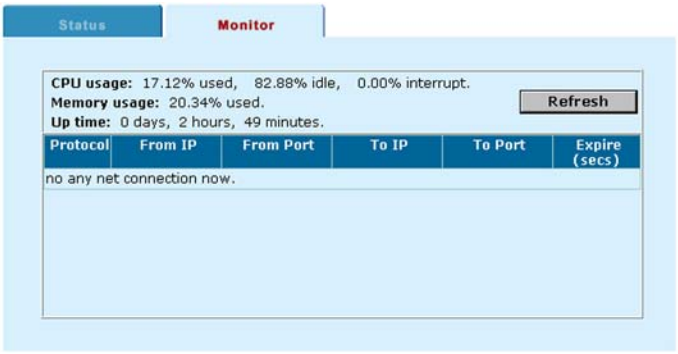
You can use the system status monitor to view system activity including the number of active connections to the DFL-500 and information about the connections. The system status monitor also displays system statistics such as CPU and memory usage.

To view system status:

- Go to *System* > *Status* > *Monitor* .

  The system status monitor display appears:
- Click Refresh to update the information displayed.

System status monitor



At the top of the display, the system status monitor shows:

CPU usage	The current CPU usage statistics of the DFL-500.
Memory usage	The percentage of available memory being used by the DFL-500.
Up time	The number of days, hours, and minutes since the DFL-500 was last started.

Each line of the system status monitor displays the following information about each active firewall connection.

Protocol	The service type or protocol of the connection.
From IP	The source IP address of the connection.
From Port	The source port of the connection.
To IP	The destination IP address of the connection.

To Port	The destination port of the connection.
Expire	The time, in seconds, before the connection expires.

Network configuration

Go to ***System > Network*** to make any of the following changes to the DFL-500 network settings:

- Changing IP addresses
- Configuring the external interface for DHCP
- Configuring the external interface for PPPoE
- Changing MTU size to improve network performance
- Setting DNS server addresses
- Controlling management access to the DFL-500
- Configuring routing
- Enabling RIP server support
- Providing DHCP services to your internal network

Changing IP addresses

- Go to *System* > *Network* > *IP Address* .
- Change the IP addresses and netmasks as required.

Configuring the external interface for DHCP

Use the following procedure to configure the DFL-500 external interface to use DHCP. This configuration is required if your ISP uses DHCP to assign the IP address of the DFL-500 external interface.

- From the web-based manager, go to ***System > Network > IP Address*** .
- Click DHCP and click OK.

The DFL-500 changes to DHCP mode and attempts to contact the DHCP server to set the external IP address, netmask, and default gateway IP address. When the DFL-500 gets this information from the DHCP server, the new addresses and netmask are displayed in the external IP address, netmask, and default gateway IP address fields. These fields are colored grey to indicate that the addresses have not been assigned manually.

Configuring the external interface for PPPoE

Use the following procedure to configure the DFL-500 external interface to use PPPoE. This configuration is required if your ISP uses PPPoE to assign the IP address of the external interface.

- Go to ***System > Network > IP Address*** .
- Click PPPoE and click OK.
- Click and type your PPPoE user name and password.
- Click OK.

The DFL-500 changes to PPPoE mode and attempts to contact the PPPoE server to set the external IP address, netmask, and default gateway IP address. When the DFL-500 gets this information from the PPPoE server, the new addresses and netmask are displayed in the external IP address, netmask, and default

gateway IP address fields. These fields are colored grey to indicate that the addresses have not been assigned manually.

Changing MTU size to improve network performance

To improve the performance of your internet connection, you can adjust the maximum transmission unit (MTU) of the packets that the DFL-500 transmits from its external interface. Ideally, you want this MTU to be the same as the smallest MTU of all the networks between your machine and the Internet. If your packets are larger, they get broken up or fragmented, which slows down transmission speeds.

Trial and error is the only sure way of finding the optimal MTU, but there are some guidelines that can help. For example, the MTU of many PPP connections is 576, so if you connect to the Internet via PPP or PPPoE, you might want to set the MTU of the DFL-500 to 576. DSL modems may also have small MTU sizes. Most ethernet networks have an MTU of 1500.

If you connect to your ISP using DHCP to obtain an IP address for the external interface, you cannot set the MTU below 576 bytes due to DHCP communication standards.

To change the MTU size of the packets leaving the external interface:

- Go to ***System > Network > IP Address*** .
- Click Fragment outgoing packets greater than MTU.
- Set the MTU size.

Set the maximum packet size in the range of 68 to 1500 bytes. The default MTU size is 1500. Experiment by lowering the MTU to find an MTU size for best network performance.

Setting DNS server addresses

Several functions of the DFL-500, including sending alert emails and URL blocking, use DNS.

To set the DNS server addresses using the web-based manager:

- Go to *System* > *Config* > *DNS* .
- Change the primary and secondary DNS server addresses as required.

Controlling management access to the DFL-500

Use the options on the Management Access page to control access to the DFL-500 web-based manager and the CLI through the Internal and External (from the Internet) interfaces. Administrators access the web-based manager using HTTPS. Administrators access the CLI remotely using SSH.

- Go to ***System > Network > Access*** .
- Check or uncheck the following parameters for each interface:

  HTTPS To allow secure connections to the web-based manager.

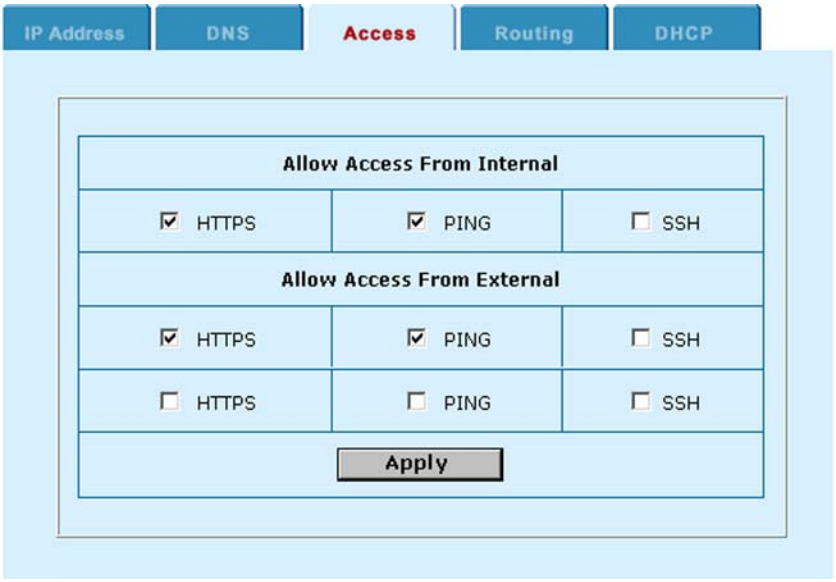
  PING If you want the DFL-500 to respond to pings. Use this setting to verify your installation and for testing.

  SSH If you want to allow secure SSH connections to the CLI.

  Checking HTTPS or SSH for the external interface allows remote administration of the DFL-500 from any location on the Internet.
- Click Apply.

You can also control the IP addresses from which administrators can access the web-based manager. See Adding and editing administrator accounts.

Setting management access



Configuring routing

If there are multiple routers installed on your network, you can configure static routes to determine the path that data follows over your network before and after it passes through the DFL-500. You can also use static routing to allow different IP domain users to access the Internet through the DFL-500.

Use the DFL-500 Routing function to add, edit, and delete static routes.

- Go to ***System > Network > Routing*** .
- Click New to add a new route.
- Define the route by specifying the destination IP address, netmask, interface, and gateway for the route.
- Click OK to save the new static route.
- To change a route, choose the route to change and click Edit .
- To delete a route, choose the route to delete and click Delete .

Enabling RIP server support

Enable RIP server support to configure the DFL-500 to act like a RIP server. The RIP routing protocol maintains up-to-date dynamic routing tables between nearby routers. You can configure RIP server support for the Internal or External interface. When activated, the DFL-500 acts like a RIP server, broadcasting RIP packets to other nearby routers to:

- Request network updates from nearby routers
- Send its own routing tables to other routers
- Announce that the DFL-500 RIP is coming online (RIP server turned on) and requesting updates
- Announce that the DFL-500 RIP is shutting down and will stop sharing routing information

To enable RIP server support:

- Go to ***System > Network > Routing*** .

- Click Internal interface to enable RIP server support from the internal interface.
- Click External interface to enable RIP server support from the external interface.

Providing DHCP services to your internal network

If it is operating in NAT mode, you can configure the DFL-500 to be the DHCP server for your internal network.

- Go to *System* > *Network* > *DNS* .
- If they have not already been added, add the primary and secondary DNS server addresses provided to you by your ISP.

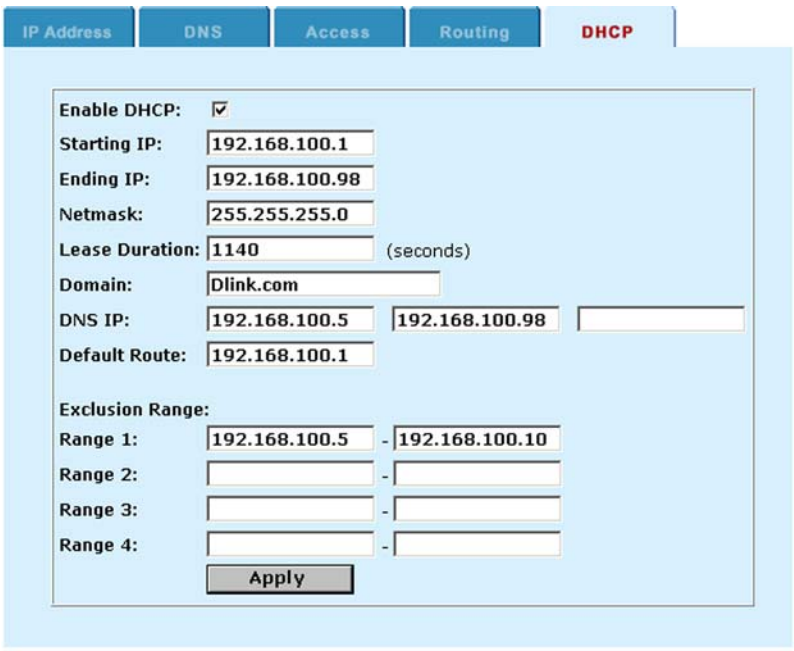
This step is not required if the external IP address of the DFL-500 is configured using DHCP or PPPoE.

- Click Apply.
- Go to ***System > Network > DHCP*** .
- Click Enable DHCP.
- Configure DHCP settings:

Starting IP **Ending IP**	If required, change the Starting IP and the Ending IP to configure the range of IP addresses that the DFL-500 can assign.
Netmask	Configure the Netmask that the DFL-500 assigns to the DHCP clients.
Lease Duration	Optionally specify the interval in minutes after which a DHCP client must ask the DHCP server for a new address.
Domain	Optionally specify the domain that the DHCP server assigns to the client.
DNS IP	Optionally specify the IP addresses of up to 3 DNS servers that the DHCP clients can use for looking up domain names.
Default Route	Optionally specify the default route assigned to DHCP clients.
Exclusion Range	Optionally specify up to 4 exclusion ranges of IP addresses within the starting IP and ending IP addresses that cannot be assigned to DHCP clients.

- Click Apply.
- Configure the IP network settings of the computers on your network to use DHCP. Use the address of the DFL-500 internal interface as the DHCP server address.

Sample DHCP settings



System configuration

Go to ***System > Config*** to make any of the following changes to the DFL-500 system configuration:

- Setting system date and time
- Changing web-based manager options
- Adding and editing administrator accounts
- Configuring SNMP

Setting system date and time

For effective scheduling and logging, the DFL-500 time should be accurate. You can either manually set the DFL-500 time, or you can configure the DFL-500 to automatically keep its time correct by synchronizing with a Network Time Protocol (NTP) server.

For more information on NTP and to find the IP address of an NTP server that you can use, see http://www.ntp.org.

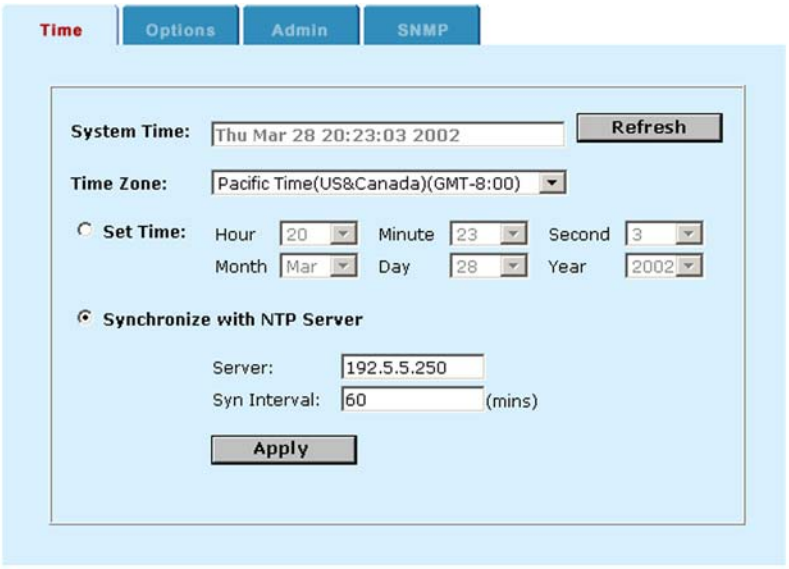
To set the date and time from the web-based manager:

- Go to *System* > *Config* > *Time* .
- Click Refresh to display the current DFL-500 date and time.
- Select your Time Zone from the list.
- Optionally, click Set Time and set the DFL-500 date and time to the correct date and time.
- To configure the DFL-500 to use NTP, click Synchronize with NTP server.

  By default, the DFL-500 is configured to connect to an NTP server at IP address 192.5.5.250, which is the IP address of an NTP server maintained by the Internet Software Consortium at Palo Alto, CA, USA.
- Optionally, enter the IP address of a different NTP server.
- Specify how often the DFL-500 should synchronize its time with the NTP server. A typical Syn Interval would be 1440 minutes for the DFL-500 to synchronize its time once a day.

- Click Apply.

Example date and time setting



Changing web-based manager options

You can change the web-based manager idle timeout, firewall user authentication timeout and character set used by the web-based manager.

- Go to *System* > *Config* > *Options* .
- Set the web-based manager idle time-out.

  Set the idle time-out to control the amount of inactive time that the web-based manager waits before requiring the administrator to log in again.

  The default idle time-out is 5 minutes. The maximum idle time-out is 480 minutes (8 hours).
- Set the firewall outgoing policy user authentication time-out.

  For more information, see Users and authentication. The default Auth time-out is 15 minutes. The maximum Auth time-out is 480 minutes (8 hours).
- Click Apply.

The options that you have selected take affect.

Adding and editing administrator accounts

When the DFL-500 is initially installed, it is configured with a single administrator account with the user name admin. From this administrator account you can add and edit administrator accounts. You can also control the access level of each of these administrative accounts and, optionally, control the IP address from which the administrator can connect to the DFL-500.

There are three administration account access levels:

admin	Has all permissions. Can view, add, edit, and delete administrator accounts. Can view and change the DFL-500 configuration. There is only one admin user.
Read & Write	Can view and change the DFL-500 configuration. Cannot view, add, edit, or delete administrator accounts. Can edit their own administrator accounts.
Read Only	Can view the DFL-500 configuration.

This section contains the following procedures:

- Adding new administrator accounts
- Editing administrator accounts

Adding new administrator accounts

From the admin account, use the following procedure to add new administrator accounts to the DFL-500 and control their permission levels.

- Go to *System* > *Config* > *Admin* .
- Click New to add an administrator account.
- Type a login name for the administrator account.
- Type and confirm a password for the administrator account.

  The password must be at least 6 characters long and can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and the @ character are not allowed.
- Optionally, specify a trusted host IP address and netmask for the location from which the administrator can log into the web-based manager.
- Set the permission level for the administrator.

Read Only	The administrator can access the web-based manager and the CLI to view the configuration but cannot change settings.
Read & Write	The administrator can view and change settings.

- Click OK to add the administrator account.

Editing administrator accounts

The admin account user can change individual administrator account passwords, configure the IP addresses from which administrators can access the web-based manager, and change the administrator's permission level.

Other administrator account users with Read & Write access can change their own administrator passwords.

To edit an administrator account:

- Go to *System* > *Config* > *Admin* .
- To change an administrator account password, click Change Password .
- Type a New Password and Confirm the new password.

  The password must be at least 6 characters long and can contain numbers (0-9) and upper and lower case letters (A-Z, a-z), and the special characters - and _. Spaces and the @ character are not allowed.
- Click OK.
- To edit the settings of an administrator account, click Edit .
- In the Trusted Host field, you can enter the IP address of the computer from which the administrator can connect to the web-based manager.
- In the Host Mask field, you can enter 255.255.255.255 if the administrator must work from just one computer.
- Change the administrator's permission as required.
- Click OK.
- To delete an administrator account, choose the account to delete and click Delete .

Configuring SNMP

Configure SNMP for the DFL-500 so that the SNMP agent running on the DFL-500 can report system information and send traps. Traps can alert system administrators about problems with the DFL-500.

- Go to *System* > *Config* > *SNMP* .
- Select Enable SNMP.
- Configure SNMP settings:

System Name	Specify a name for this DFL-500.
System Location	Describe the physical location of the DFL-500.
Contact Information	Add the contact information for the person responsible for this DFL-500.
Get Community	Also called read community, get community acts like a password to identify SNMP get requests sent from the DFL-500. The DFL-500 sends the get community string with each SNMP get request. The same get community string must be added to the SNMP monitoring software to allow communication with the DFL-500. The default get community string is "public". Specify a community string to keep intruders from accessing get requests to retrieve information about your network configuration.
Trap Community	The trap community string functions like a password that is sent along with SNMP traps. Change the trap community string to keep intruders from accessing traps. The same trap community string must be added to the SNMP monitoring software.
First Trap Receiver IP Address	Optionally specify the IP address of the SNMP monitor to which to send traps.
Second Trap Receiver IP Address	Optionally specify the IP address of a second SNMP monitor to which to send traps.
Third Trap Receiver IP Address	Optionally specify the IP address of a third SNMP monitor to which to send traps.

- Click Apply.

Sample SNMP configuration

Using the DFL-500 CLI

The command line interface (CLI) is intended as a troubleshooting tool to help diagnose and fix system problems that cannot be solved from the web-based manager.

This chapter explains how to connect to the DFL-500 CLI and also describes some of the basics of using the CLI. You can use CLI commands to view all system information and to change all system configuration settings.

This chapter describes:

- Connecting to the DFL-500 CLI
- CLI basics
- Installing firmware from a TFTP server

Connecting to the DFL-500 CLI

There are two methods to connect to the DFL-500 CLI:

- Connecting to the DFL-500 communications port
- Connecting to the DFL-500 CLI using SSH

Connecting to the DFL-500 communications port

To connect to the DFL-500 CLI through the communications port you require:

- A computer with an available communications port
- A null modem cable with a 9-pin connector to connect to the communications port on the back panel of the DFL-500
- Terminal emulation software such as HyperTerminal for Windows

The following procedure describes how to connect to the DFL-500 CLI using Windows HyperTerminal software. You can use any terminal emulation program.

To connect to the DFL-500 CLI:

- Connect the null modem cable to the communications port of your computer and to the communications port on the back of the DFL-500.
- Make sure the DFL-500 is powered on.
- Start HyperTerminal, enter a name for the connection, and click OK.
- Specify the communications port in the Connect using field and click OK.
- Select the following port settings and click OK:
    - Bits per second: 9600
    - Data bits: 8
    - Parity: None
    - Stop bits: 1
    - Flow control: None
- Press Enter to connect to the DFL-500 CLI.

  The following prompt appears:

  ```
  D-Link login:
  ```
- Type a valid administrator name and press Enter.

- Type the password for this administrator and press Enter.
  The following prompt appears:
  ```
  Type ? for a list of commands.
  ```

Connecting to the DFL-500 CLI using SSH

SSH provides strong secure authentication and secure communications to the DFL-500 CLI over your internal network or the Internet. Once the DFL-500 is configured to accept SSH connections, you can run an SSH client on your management computer and use this client to connect to the DFL-500 CLI.

Accepting SSH connections

To use the web-based manager to configure the DFL-500 to accept SSH connections, see Controlling management access to the DFL-500.

The following procedure describes how to use the CLI to configure the DFL-500 to accept SSH connections:

- Connect to the CLI using the DFL-500 communications port and your terminal emulation software.
- To configure the internal interface to accept SSH connections. Enter:
  ```
  set system access internal ssh enable
  ```
- To configure the external interface to accept SSH connections. Enter:
  ```
  set system access external ssh enable
  ```
- To confirm that you have configured SSH access correctly, enter the following command to view the access settings for all of the interfaces:
  ```
  get system access
  ```
  The following response shows that you can connect to the internal interface using SSH as well as HTTPS, that you can connect to the external interface using SSH, and that all of the interfaces will respond to a ping request.
  ```
  internal: HTTPS,PING,SSH
  external: PING,SSH
  ```

Connecting to the CLI using SSH

To connect to the CLI using SSH you must install an SSH client.

- Start the SSH client and connect to a DFL-500 interface that is configured for SSH connections.
  The following prompt appears:
  ```
  D-Link login:
  ```
- Type a valid administrator name and press Enter.
- Type the password for this administrator and press Enter.
  The following prompt appears:
  ```
  Type ? for a list of commands.
  ```
  You have connected to the DFL-500 CLI, and you can proceed to enter CLI commands as if you have connected through the DFL-500 communications port.

CLI basics

This section describes the basics of using the DFL-500 CLI to enter commands.

Recalling commands

You can recall commands by using the Up and Down arrow keys to cycle through commands you have entered.

Editing commands

Use the Left and Right arrow keys to move the cursor back and forth on the command line. Use the Backspace and Delete keys to edit the command. You can also use control keys to edit commands. Control keys for editing commands lists control keys for editing commands.

Control keys for editing commands

Function	Key combination
Beginning of line	CTRL+A
End of line	CTRL+E
Back one character	CTRL+B
Forward one character	CTRL+F
Delete current character	CTRL+D
Previous command	CTRL+P
Next command	CTRL+N
Abort line	CTRL+C

Using command shortcuts

You can abbreviate commands and command options to the smallest number of non ambiguous characters. For example, the command `get system status` can be abbreviated to `g sy st`.

Using command help

You can press the tab key or the question mark (?) key to display command help.

- Press the tab key or the question mark (?) key at the command prompt to display a list of the commands available and a description of each command
- Type a command followed by a space and press the tab key or the question mark (?) key to display a list of the options available for that command and a description of each option
- Type a command followed by an option and press the tab key or the question mark (?) key to display a list of additional options available for that command option combination and a description of each option

Installing firmware from a TFTP server

D-Link releases new versions of the DFL-500 firmware periodically. When D-Link releases new firmware, you can download the upgrade from our Web site (http://tsd.dlink.com.tw). You can save this file on your management computer and then use the following procedure to upgrade the firmware on your DFL-500.

This procedure deletes all of the changes that you have made to the DFL-500 configuration and reverts the system to its default configuration, including resetting interface addresses. Before installing new firmware make sure you download your configuration file, see Backing-up system settings.

You can also upgrade the DFL-500 from the web-based manager (see Upgrading the DFL-500 firmware).

To install a firmware upgrade using the CLI:

- Configure a TFTP server on one of the computers on your internal network.
  The TFTP server should be on the same subnet as the internal interface of the DFL-500.
  You can download a TFTP server from:
  http://site.ifrance.com/freewares/P_tftpd32.htm.
- Make sure the TFTP server is running.
- Make sure the Internal interface of the DFL-500 is connected to your internal network.
- To confirm that you can connect to the TFTP server from the DFL-500, start the DFL-500 CLI and use the following command to ping the computer running the TFTP server. If the TFTP server's IP address is 192.168.1.168:
  ```
  > diagnose ping 192.168.1.168
  ```
- Copy the new firmware image file to the root directory of your TFTP server.
- Cycle the power on the DFL-500.
  As the DFL-500 powers back up, messages similar to the following appear in the CLI session window:
  ```
  BIOS Version 2.2
  Serial number: FGT-502801012243
  SDRAM Initialization.
  Scanning PCI Bus...Done.
  Total RAM: 256M
  Enabling Cache...Done.
  Allocating PCI Resources...Done.
  Zeroing IRQ Settings...Done.
  Enabling Interrupts...Done.
  Configuring L2 Cache...Done.
  Boot Up, Boot Device Capacity=62592k Bytes.
  Press Any Key To Download Boot Image.
  ...
  ```
- Quickly press any key to interrupt system startup.
  The following message appears:
  ```
  Enter TFTP Server Address [192.168.1.168]:
  ```
- Type the address of the TFTP server and press Enter.
  The following message appears:
  ```
  Enter Local Address [192.168.1.188]:
  ```
- Type the address of the internal interface of the DFL-500 and press Enter.
  The following message appears:
  ```
  Enter File Name [image.out]:
  ```
- Enter the firmware image file name and press Enter.
  The TFTP server uploads the firmware image file to the DFL-500 and messages similar to the following appear:
  ```
  Total 7682959 Bytes Data Is Downloaded.
  Testing The Boot Image Now.
  ```

```
Total 32768k Bytes Are Unzipped.
Do You Want To Save The Image ?[Y/n]
```

Type `Y`.

```
Programming The Boot Device Now.
.................................
Read Boot Image 548405 Bytes.
Initializing Firewall ...

D-Link Login:
```

The installation can take a few minutes to complete.

You must then restore your previous configuration. Begin by changing the interface addresses. You can do this from the CLI using the command:

```
set system interface
```

Once the interface addresses are changed you can access the DFL-500 from the web-based manager and upload your configuration files.

Glossary

Connection : A link between machines, applications, processes, etc. that can be logical, physical, or both.

DNS, Domain Name Service : A service that converts symbolic node names to IP addresses.

Ethernet : A local-area network (LAN) architecture that uses a bus or star topology and supports data transfer rates of 10 Mbps. Ethernet is one of the most widely implemented LAN standards. A newer version of Ethernet, called 100Base-T (or Fast Ethernet), supports data transfer rates of 100 Mbps. And the newest version, Gigabit Ethernet supports data rates of 1 gigabit (1,000 megabits) per second.

External interface : The DFL-500 interface that is connected to the Internet.

FTP, File transfer Protocol : An application and TCP/IP protocol used to upload or download files.

Gateway : A combination of hardware and software that links two different types of networks. Gateways between TCP/IP networks, for example, can link different subnetworks.

HTTP, Hyper Text Transfer Protocol : The protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

HTTPS : The SSL protocol for transmitting private documents over the Internet using a Web browser.

Internal interface : The DFL-500 interface that is connected to your internal (private) network.

Internet : A collection of networks connected together that span the entire globe using the NFSNET as their backbone. As a generic term, it refers to any collection of interdependent networks.

ICMP, Internet Control Message Protocol : Part of the Internet Protocol (IP) that allows for the generation of error messages, test packets, and information message relating to IP. This is the protocol used by the ping function when sending ICMP Echo Requests to a network host.

IKE, Internet Key Exchange : A method of automatically exchanging keys between two secure servers.

IMAP, Internet Message Access Protocol : An Internet email protocol that allows access to your email from any IMAP compatible browser. With IMAP, your mail resides on the server.

IP, Internet Protocol : The component of TCP/IP that handles routing.

IP Address : An identifier for a computer or device on a TCP/IP network. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255.

L2TP, Layer Two (2) Tunneling Protocol : An extension to the PPP protocol that enables ISPs to operate Virtual Private Networks (VPNs). L2TP merges PPTP from Microsoft and L2F from Cisco Systems. To create a L2TP VPN your ISP's routers must support L2TP.

IPSec, Internet Protocol Security : A set of protocols that support secure exchange of packets at the IP layer. IPSec is most often used to support VPNs.

LAN, Local Area Network : A computer network that spans a relatively small area. Most LANs connect workstations and personal computers. Each computer in a LAN is able to access data and devices anywhere on the LAN. This means that many users can share data and resources such as printers.

MAC address : Media Access Control address, a hardware address that uniquely identifies each node of a network.

Modem : A device that converts digital signals into analog signals and back again for transmission over telephone lines.

MTU , ***Maximum Transmission Unit*** : The largest physical packet size, measured in bytes, that a network can transmit. Any packets larger than the MTU are divided into smaller packets before being sent. Ideally, you want the MTU your network produces to be the same as the smallest MTU of all the networks between your machine and a message's final destination. If your messages are larger than one of the intervening MTUs, they get broken up (fragmented), which slows down transmission speeds.

Netmask : Also called subnet mask. A set of rules for omitting parts of a complete IP address to reach a target destination without using a broadcast message. It can indicate a subnetwork portion of a larger network in TCP/IP. Sometimes referred to as an Address Mask.

NTP , ***Network Time Protocol*** : Used to synchronize the time of a computer to an NTP server. NTP provides accuracies within a tens of milliseconds across the Internet relative to Coordinated Universal Time (UTC).

Packet : A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called datagrams.

Ping, Packet Internet Grouper : A utility used to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply.

POP3, Post Office Protocol : A protocol used to retrieve e-mail from a mail server to a mail client across the Internet. Most e-mail clients use the POP protocol.

PPP, Point-to-Point Protocol : A TCP/IP protocol that provides host-to-network and router-to-router connections.

PPTP, Point-to-Point Tunneling Protocol : A Windows-based technology for creating VPNs. PPTP is supported by Windows 98, 2000, and XP. To create a PPTP VPN your ISP's routers must support PPTP.

Port : In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

Protocol : An agreed-upon format for transmitting data between two devices. The protocol determines the type of error checking to be used, the data compression method (if any), how the sending device indicates that it has finished sending a message, and how the receiving device indicates that it has received a message.

RADIUS , ***Remote Authentication Dial-In User Service*** : An authentication and accounting system used by many Internet Service Providers (ISPs). When users dial into an ISP they enter a user name and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.

Router : A device that connects LANs into an internal network and routes traffic between them.

Routing : The process of determining a path to use to send data to its destination.

Routing table : A list of valid paths through which data can be transmitted.

SCCU , ***Security and Content Control Units*** : D-Link products that provide high-performance, hardware-based protection against content-based security threats, such as viruses and worms, combined with firewall, VPN, intrusion detection, content filtering, and traffic shaping.

Server : An application that answers requests from other devices (clients). Used as a generic term for any device that provides services to the rest of the network such as printing, high capacity storage, and network access.

SSH , ***Secure shell*** : A secure Telnet replacement that you can use to log into another computer over a network to run commands. SSH provides strong secure authentication and secure communications over insecure channels.

SMTP, Simple Mail Transfer Protocol : In TCP/IP, this is an application for providing mail delivery services.

SNMP , ***Simple Network Management Protocol*** : A set of protocols for managing networks. SNMP works by sending messages to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

Subnet : A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 100.100.100. would be part of the same subnet. Dividing a network into subnets is useful for both security and performance reasons. IP networks are divided using a subnet mask.

Subnet Address : The part of the IP address that identifies the subnetwork.

TCP, Transmission Control Protocol : One of the main protocols in TCP/IP networks. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

UDP, User Datagram Protocol : A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP, UDP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It's used primarily for broadcasting messages over a network.

VPN, Virtual Private Network : A network that links private networks over the Internet. VPNs use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

Virus : A computer program that attaches itself to other programs, spreading itself through computers or networks by this mechanism usually with harmful intent.

Worm : A program or algorithm that replicates itself over a computer network, usually through email, and performs malicious actions, such as using up the computer's resources and possibly shutting the system down.

Troubleshooting FAQs

The following troubleshooting FAQs are available:

- General administration
- Network configuration
- Firewall policies
- Schedules
- VPN
- Virus protection
- Web content filtering
- Logging

General administration

Q: I am trying to set up some of the firewall options, but it keeps asking me for a password while I work.

See Changing web-based manager options.

Q: I can't find the administrator pages on the firewall.

See Logging into the web-based manager. Use the front panel Keypad to check the IP address of the interface to which you are trying to connect.

Q: Administration from the Internet does not work.

See Controlling management access to the DFL-500.

Q: Everyone in the world knows the password.

See Adding and editing administrator accounts.

Q: I just spent a week setting up and things are working perfectly. Is there some way to save the configuration before making any more changes.

See Backing-up system settings and Restoring system settings.

Q: How can I get a warning when someone is attacking my network?

See Alert email.

Network configuration

Q: I am trying to set up the network connections, but I can't seem to ping the firewall.

See Controlling management access to the DFL-500.

Firewall policies

Q: When I set policies all the computers on the network seem to be affected. The policy for a single machine is being applied to the entire network.

This most often occurs when adding a single address and forgetting to change the netmask from 255.255.255.0 to 255.255.255.255.

Q: My policies are set correctly but I still cannot connect to the Internet from one or more of the computers on my internal network.

Check the default gateway setting on that particular computer. Its default gateway must match the internal address of the DFL-500.

Q: I checked the default gateway and it matches but I still cannot connect to the Internet.

Make sure that the external address and external gateway of the firewall have been properly set to your Internet Service Provider's (ISP) specifications. If there is no discrepancy, it would be a good idea to double check with your ISP that they have provided you with the correct information.

Q: I am having problems setting up my outgoing and incoming policies. The external or internal addresses cannot be entered in the destination or source lists.

When setting up incoming or outgoing policies, it is important to remember that new addresses cannot be entered into the Destination or Source fields. New addresses (external or internal) must be added manually into the external or internal address lists. The choices under the Destination and Source menus come directly from the address lists.

Q: I want to set up an incoming policy for an FTP server on my internal network, but the destination address list for incoming policies shows only external addresses.

Before creating an incoming policy you need to set up a valid Internet address so that it can be used to connect to your FTP server. This external address can then be used as the destination in an incoming policy. See Controlling connections from the Internet.

Q: I want to connect to a TELNET/FTP/WEB server across the Internet. If I set the outgoing policy service field to TELNET/FTP/HTTP I can't connect.

Try setting the service to ANY. Settings for individual services assume that the standard port for that service is being used, and only traffic addressed to that port is allowed through. If you are using a non-standard port this will not work. ANY allows traffic to go to all ports.

Schedules

Q: I need a schedule that will allow access to the Internet overnight, from 9:00 pm to 9:00 am. How can I do this?

There are two ways:

- Use two policies with two schedules, one from 9:00 pm to midnight, and one from midnight to 9:00 am.
- Create a policy allowing access for the whole day, then add another one before it in the policy list denying access from 9:00 am to 9:00 pm.

VPN

Q: The client to subnet configuration was working, but now it has shut down and I can't recover. How do I get it back again?

This happens when the tunnel is down and the client software thinks it is still connected. To recover you must disconnect at the client end.

Q. Why can't I bring up the connection in the case of subnet to subnet configuration?

First check whether you have set up the proper IPSec policy for this connection. If you have, check whether the authentication keys are same on the local and remote IPSec gateways. Also check whether the remote gateway address is correct.

Virus protection

Q: I am worried about viruses so I set the Anti-Virus options to the highest level. Now people are complaining that some files that they need are blocked.

When Anti-Virus protection for HTTP or any of the email protocols is set to high, all files of potentially dangerous types are blocked. The simple cure for this problem is to set a lower Security Protection Level. Under normal conditions, all of the Anti-Virus Security Protection Levels can safely be set to Medium. High security should only be used in extreme circumstances when a new virus has been found.

Q: A new virus is spreading through the Internet. What should I do?

Set virus protection to high. See High level virus protection for your internal network. Next contact D-Link and obtain an AntiVirus database update which includes the new virus. To install the new database, see Updating your antivirus database.

Web content filtering

Q: My employees are job hunting on the Internet when they should be working. Is it possible to block the career sites.

See Block access to Internet sites and enter the names of the offending sites into the URL block list.

Q: I am worried about dangerous web content so I set the Script Filter options to block all scripts, Java Applets, ActiveX, and cookies. Now people are complaining that some web sites are inaccessible or don't work properly.

Some of the content types that can be blocked on the ***Web Filter > Script Filter*** page may be required for a few Internet sites to work properly.

Logging

Q: I want to keep track of any attempts by intruders to go through the firewall to our network or to get control of the firewall.

Go to ***Log & Report > Log Setting*** and turn on Log All External Traffic To Firewall. All attempts to access the firewall are recorded. You can also get email alert messages by going to ***System > Config > Alert Mail*** and entering the necessary information.

Q: Can I identify the attackers from the log?

The log does contain the IP address that the violating packets originated from, but since most Internet users do not have static IP addresses these may not provide all of the information that you need.

Q: Our web site is on a computer on the internal network. How can I tell how many people look at it?

Go to ***Log & Report > Log Setting*** and turn on Log All Incoming Policy Traffic. All traffic from the Internet to the local network are recorded.

Q: How can I find out which company employees are spending time on the Internet?

Go to ***Log & Report > Log Setting*** and turn on Log All Outgoing Policy Traffic. All connections to Internet sites are logged.

Q: I would like to use remote logging to my administration computer. How do I set up a syslog server?

Several freeware syslog servers for Microsoft Windows and other operating systems are available on the Internet, and most can be very easily set up. In some cases a more advanced commercial version is available for a modest fee.

Technical Support

D-Link® Offices

AUSTRALIA
D-LINK AUSTRALIA
Unit 16, 390 Eastern Valley Way, Roseville, NSW 2069, Australia
TEL: 61-2-9417-7100 FAX: 61-2-9417-1077
TOLL FREE: 1800-177-100 (Australia), 0800-900900 (New Zealand)
E-MAIL: support@dlink.com.au, info@dlink.com.au URL: www.dlink.com.au

BENELUX
D-LINK BENELUX
Fellenoord 130, 5611 ZB Eindhoven, The Netherlands
TEL: 31-40-2668713 FAX: 31-40-2668666
E-MAIL:info@dlink-benelux.nl, info@dlink-benelux.be URL: www.dlink-benelux.nl/, www.dlink-benelux.be/

CANADA
D-LINK CANADA
#2180 Winston Park Drive, Oakville, Ontario, L6H 5W1 Canada
TEL: 1-905-829-5033 FAX: 1-905-829-5095 FREE CALL: 1-800-354-6522
E-MAIL: techsup@dlink.ca URL: www.dlink.ca FTP: ftp.dlinknet.com

CHILE
D-LINK SOUTH AMERICA
Isidora Goyeechea 2934 of 702, Las Condes, Santiago – Chile S.A.
TEL: 56-2-232-3185 FAX: 56-2-232-0923
E-MAIL: ccasassu@dlink.cl, tsilva@dlink.cl URL: www.dlink.cl

CHINA
D-LINK CHINA
2F., Sigma Building, 49 Zhichun Road, Haidian District, 100080 Beijing, China
TEL: 86-10-88097777 FAX: 86-10-88096789

DENMARK
D-LINK DENMARK
Naverland 2, DK-2600 Glostrup, Copenhagen, Denmark
TEL:45-43-969040 FAX:45-43-424347
E-MAIL: info@dlink.dk URL: www.dlink.dk

EGYPT
D-LINK MIDDLE EAST
7 Assem Ebn Sabet Street, Heliopolis Cairo, Egypt
TEL: 202-2456176 FAX: 202-2456192
E-MAIL: support@dlink-me.com URL: www.dlink-me.com

FINLAND
D-Link FINLAND
Thlli-ja Pakkahuone Katajanokanlaituri 5, FIN-00160 Helsinki, Finland
TEL: 358-9-622-91660 FAX: 358-9-622-91661
E-MAIL: info@dlink-fi.com URL: www.dlink-fi.com

FRANCE
D-LINK FRANCE
Le Florilege #2, Allee de la Fresnerie, 78330 Fontenay le Fleury France
TEL: 33-1-302-38688 FAX: 33-1-3023-8689
E-MAIL: info@dlink-france.fr URL: www.dlink-france.fr

GERMANY
D-LINK Central Europe/D-Link Deutschland GmbH
Schwalbacher Strasse 74, D-65760 Eschborn, Germany
TEL: 49-6196-77990 FAX: 49-6196-7799300
INFO LINE: 00800-7250-0000 (toll free) HELP LINE: 00800-7250-4000 (toll free)
REPAIR LINE: 00800-7250-8000
E-MAIL: info@dlink.de URL: www.dlink.de

IBERIA
D-LINK IBERIA
Gran Via de Carlos III, 84, 3˚ Edificio Trade, 08028 BARCELONA
TEL. 34 93 4090770 FAX 34 93 4910795
E-MAIL: info@dlinkiberia.es URL: www.dlinkiberia.es

INDIA
D-LINK INDIA
Plot No.5, Kurla-Bandra Complex Road, Off Cst Road, Santacruz (E), Bombay - 400 098 India
TEL: 91-22-652-6696 FAX: 91-22-652-8914
E-MAIL: service@dlink.india.com URL: www.dlink-india.com

ITALY
D-LINK ITALIA
Via Nino Bonnet No. 6/b, 20154 Milano, Italy
TEL: 39-02-2900-0676 FAX: 39-02-2900-1723
E-MAIL: info@dlink.it URL: www.dlink.it

JAPAN
D-LINK JAPAN
10F, 8-8-15 Nishi-Gotanda, Shinagawa-ku, Tokyo 141, Japan
TEL: 81-3-5434-9678 FAX: 81-3-5434-9868
E-MAIL: kida@d-link.co.jp URL: www.d-link.co.jp

NORWAY
D-LINK NORWAY
Waldemar Thranesgt. 77, 0175 Oslo, Norway
TEL: 47-22-991890 FAX: 47-22-207039

RUSSIA
D-LINK RUSSIA
Michurinski Prospekt 49, 117607 Moscow, Russia
TEL: 7-095-737-3389, 7-095-737-3492 FAX: 7-095-737-3390
E-MAIL: vl@dlink.ru URL: www.dlink.ru

SINGAPORE
D-LINK INTERNATIONAL
1 International Business Park, #03-12 The Synergy, Singapore 609917
TEL: 65-774-6233 FAX: 65-774-6322
E-MAIL: info@dlink.com.sg URL: www.dlink-intl.com

S. AFRICA
D-LINK SOUTH AFRICA
102-106 Witchhazel Avenue, Einetein Park 2, Block B, Highveld Technopark Centurion, South Africa
TEL: 27(0)126652165 FAX: 27(0)126652186
E-MAIL: attie@d-link.co.za URL: www.d-link.co.za

SWEDEN
D-LINK SWEDEN
P.O. Box 15036, S-167 15 Bromma Sweden
TEL: 46-(0)8564-61900 FAX: 46-(0)8564-61901
E-MAIL: info@dlink.se URL: www.dlink.se

TAIWAN
D-LINK TAIWAN
2F, No. 119 Pao-Chung Road, Hsin-Tien, Taipei, Taiwan,
TEL: 886-2-2910-2626 FAX: 886-2-2910-1515
E-MAIL: dssqa@tsc.dlinktw.com.tw URL: www.dlinktw.com.tw

U.K.
D-LINK EUROPE
4th Floor, Merit House, Edgware Road, Colindale, London, NW9 5AB, U.K.
TEL: 44-20-8731-5555 FAX: 44-20-8731-5511
E-MAIL: info@dlink.co.uk URL: www.dlink.co.uk

U.S.A.
D-LINK U.S.A.
53 Discovery Drive, Irvine, CA 92618 USA
TEL: 1-949-788-0805 FAX: 1-949-753-7033 INFO LINE: 1-800-326-1688
BBS: 1-949-455-1779, 1-949-455-9616
E-MAIL: tech@dlink.com, support@dlink.com URL: www.dlink.com

Registration Card

Print, type or use block letters.

Your name: Mr./Ms _____

Organization: _____ Dept. _____

Your title at organization: _____

Telephone: _____ Fax:_____

Organization's full address: _____

_____

Country: _____

Date of purchase (Month/Day/Year): _____

Product Model	Product Serial No.	* Product installed in type of computer (e.g., Compaq 486)	* Product installed in computer serial No.

(* Applies to adapters only)

Product was purchased from:

Reseller's name: _____

Telephone: _____ Fax:_____

Reseller's full address: _____

_____

_____

Answers to the following questions help us to support your product:

1. Where and how will the product primarily be used?

☐Home ☐Office ☐Travel ☐Company Business ☐Home Business ☐Personal Use

2. How many employees work at installation site?

☐1 employee ☐2-9 ☐10-49 ☐50-99 ☐100-499 ☐500-999 ☐1000 or more

3. What network protocol(s) does your organization use ?

☐XNS/IPX ☐TCP/IP ☐DECnet ☐Others_____

4. What network operating system(s) does your organization use ?

☐D-Link LANsmart ☐Novell NetWare ☐NetWare Lite ☐SCO Unix/Xenix ☐PC NFS ☐3Com 3+Open
☐Banyan Vines ☐DECnet Pathwork ☐Windows NT ☐Windows NTAS ☐Windows '95
☐Others_____

5. What network management program does your organization use ?

☐D-View ☐HP OpenView/Windows ☐HP OpenView/Unix ☐SunNet Manager ☐Novell NMS
☐NetView 6000 ☐Others_____

6. What network medium/media does your organization use ?

☐Fiber-optics ☐Thick coax Ethernet ☐Thin coax Ethernet ☐10BASE-T UTP/STP
☐100BASE-TX ☐100BASE-T4 ☐100VGAnyLAN ☐Others_____

7. What applications are used on your network?

☐Desktop publishing ☐Spreadsheet ☐Word processing ☐CAD/CAM
☐Database management ☐Accounting ☐Others_____

8. What category best describes your company?

☐Aerospace ☐Engineering ☐Education ☐Finance ☐Hospital ☐Legal ☐Insurance/Real Estate ☐Manufacturing
☐Retail/Chainstore/Wholesale ☐Government ☐Transportation/Utilities/Communication ☐VAR
☐System house/company ☐Other_____

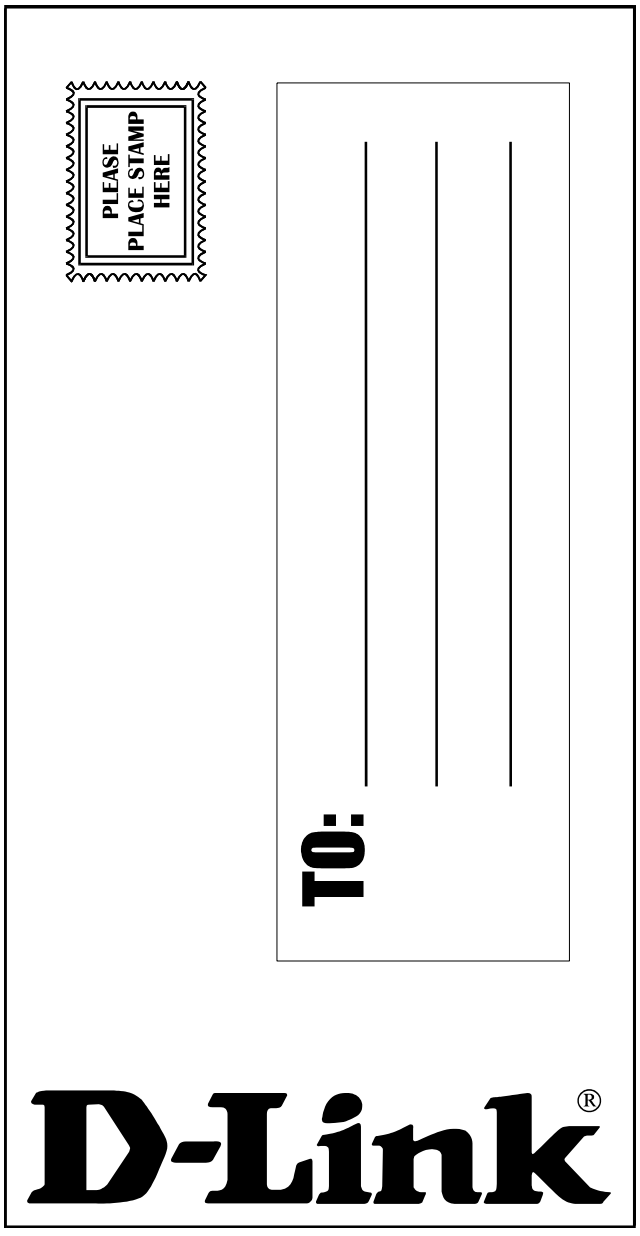
9. Would you recommend your D-Link product to a friend?

☐Yes ☐No ☐Don't know yet

10.Your comments on this product?

_____

_____


PLEASE
PLACE STAMP
HERE
TO:
D-Link®